Calhoun: The NPS Institutional Archive

DSpace Repository

Theses and Dissertations | 1. Thesis and Dissertation Collection, all items

1999

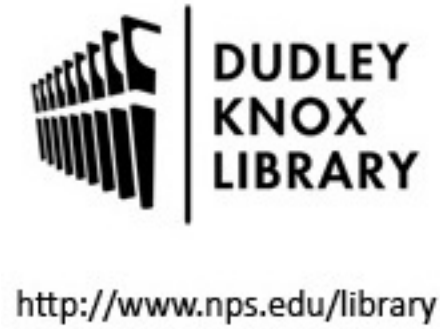
Microsoft operating systems development and strategy : an assessment of the Windows 2000 Server operating system

Oakes, David R.

Monterey, California: Naval Postgraduate School

http://hdl.handle.net/10945/13712

Downloaded from NPS Archive: Calhoun



http://www.nps.edu/library

Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

MICROSOFT OPERATING SYSTEMS DEVELOPMENT AND STRATEGY: AN ASSESSMENT OF THE WINDOWS 2000 SERVER OPERATING SYSTEM

by

David R. Oakes

September 1999

Principal Advisor: Doug Brinkley
Second Reader: James B. Michael

Approved for public release; distribution is unlimited.

DTIC QUALITY INSPECTED 4

19991026 125

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	September 1999	Master's Thesis

4. TITLE AND SUBTITLE
MICROSOFT OPERATING SYSTEMS DEVELOPMENT AND STRATEGY: AN ASSESSMENT OF THE WINDOWS 2000 SERVER OPERATING SYSTEM

5. FUNDING NUMBERS

6. AUTHOR(S)
Oakes, David R.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING/ MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES
The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)
Microsoft began development of Windows NT in the late 1980s as an applied research and development project. Since then it has become the number one network operating system on the market. With the release of Windows 2000, Microsoft has followed through on its strategy of operating system consolidation and formed a new family of servers. The Windows 2000 Server Family is the next generation of Windows NT and consolidates many of the features of Windows 95/98 into its operating system. This thesis examines the history of Microsoft and its strategy leading to the development of Windows 2000. It investigates the Windows 2000 Server Family editions, features and technologies introduced in the operating system. Then, methods of preparing an existing network for the deployment or migration to Windows 2000 are provided. A discussion of network security issues and features introduced by Windows 2000 is provided. This study provides IT managers with the background knowledge required to assess implementation issues surrounding Windows 2000.

14. SUBJECT TERMS
Windows 2000, Network, Active Directory, Microsoft Management Console, Computer Security, Kerberos Authentication Protocol, Internet Security, Public Key Infrastructure

15. NUMBER OF PAGES
167

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

Approved for public release; distribution is unlimited.

MICROSOFT OPERATING SYSTEMS DEVELOPMENT AND STRATEGY: AN ASSESSMENT OF THE WINDOWS 2000 SERVER OPERATING SYSTEM

David R. Oakes
Lieutenant, United States Navy
B.S., University of Southern Mississippi, 1985

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF SCIENCE IN SYSTEMS TECHNOLOGY
(SCIENTIFIC AND TECHNICAL INTELLIGENCE)**

from the

NAVAL POSTGRADUATE SCHOOL
September 1999

Author: [redacted]
David R. Oakes

Approved by: [redacted]
Doug Brinkley, Principal Advisor

[redacted]
James B. Michael, Second Reader

[redacted]
Daniel Boger, Chairman
C3 Academic Group

ABSTRACT

Microsoft began the development of Windows NT in the late 1980s as an applied research and development project. Since then it has become the number one network operating system on the market. With the release of Windows 2000, Microsoft has followed through on its strategy of operating system consolidation and formed a new family of servers. The Windows 2000 Server Family is the next generation of Windows NT and consolidates many of the features of Windows 95/98 into its operating system. This thesis examines the history of Microsoft and its strategy leading to the development of Windows 2000. It investigates the Windows 2000 Server Family editions, features and technologies introduced in the operating system. Then, methods of preparing an existing network for the deployment or migration to Windows 2000 are provided. A discussion of network security issues and features introduced by Windows 2000 is provided. This study provides IT decisionmakers with the background knowledge required to assess implementation issues surrounding Windows 2000.

TABLE OF CONTENTS

I. INTRODUCTION 1

A. BACKGROUND 1

B. PURPOSE 3

C. ORGANIZATION 3

II. MICROSOFT HISTORY AND STRATEGY 5

A. MS-DOS AND LAN MANAGER 5

B. WINDOWS AND WINDOWS NT 6

C. MICROSOFT'S STRATEGY OF A UNIVERSAL WINDOWS 10

1. Windows NT Workstation Leads the Way 13

2. Windows NT Server and Windows 2000 14

D. CHAPTER SUMMARY 15

III. WINDOWS 2000 SERVER EDITIONS AND FEATURES 17

A. WINDOWS 2000 SERVER EDITIONS 17

1. Windows 2000 Server Standard Edition 19

2. Windows 2000 Advanced Server 20

3. Windows 2000 Datacenter Server 23

B. WINDOWS 2000 FEATURES 25

1. Active Directory 25

2. Microsoft Management Console 36

3. Microsoft Cluster Server 46

4. Distributed File System 49

5. NT File System (NTFS) 59

C. CHAPTER SUMMARY 62

IV. PREPARING FOR WINDOWS 2000 63

A. RESTRUCTURE EXISTING DOMAINS 63

1. Downlevel Domain Models 64

2. Restructuring Options 69

B. DESIGNING WINDOWS 2000 NETWORKS 73
1. Designing the Active Directory 73
2. Planning a Dynamic DNS Structure 77
3. Hardware Needs 83
C. DEPLOYING WINDOWS 2000 86
1. Upgrade Paths for Windows 2000 87
2. Single Machine Installation 88
3. Deploying Large Sites 90
4. Migrating to Windows 2000 93
D. CHAPTER SUMMARY 97
V. WINDOWS 2000 SECURITY FEATURES 99
A. ACTIVE DIRECTORY AND SECURITY 100
1. Active Directory and Security Services 102
2. Securing Active Directory 104
3. Security Tools 106
B. THE KERBEROS AUTHENTICATION PROTOCOL 107
1. Understanding the Kerberos Authentication Protocol 107
2. Authentication Using the Kerberos Protocol 108
3. Improved Network Performance 110
4. Single Sign-on in Windows 2000 Networks 111
5. Kerberos Weaknesses 112
C. INTERNET SECURITY AND PUBLIC-KEY INFRASTRUCTURE 113
1. Overview of Public-key Cryptography and PKI 114
2. Windows 2000 PKI 116
D. CHAPTER CONCLUSION 118
VI. CONCLUSION 119
APPENDIX A. A COMPARISON OF WINDOWS NT SERVER 4.0 AND WINDOWS 2000 SERVER FAMILY FEATURES 121
APPENDIX B. MICROSOFT MANAGEMENT CONSOLE SNAP-INS 137
APPENDIX C. GLOSSARY OF TERMS AND ACRONYMS 143

LIST OF REFERENCES 151
INITIAL DISTRIBUTION LIST 155

I. INTRODUCTION

Microsoft began developing Windows NT in 1987 as a follow-on to Microsoft LAN Manager and as an alternative to IBM's OS/2. Since then, Windows NT has emerged as one of the leading technologies in server operating systems. This thesis examines the development of the newest Microsoft operating system, named the Windows 2000 Server family, and the new technologies and features introduced in the operating system.

To date, Microsoft has released the Windows 2000 B3 version and expects the final version to be released in late 1999 (latest target date is October 1999). This thesis explores Microsoft's strategy to consolidate operating systems and examines the process of preparing a new or existing network for migration to Windows 2000.

A. BACKGROUND

Microsoft began development of Windows NT (NT stands for New Technology) in the late 1980's as a result of the breakup of its partnership with IBM. This breakup prompted Microsoft to focus on Windows rather than IBM's OS/2. Windows NT was first released in 1993 after several years of design and development. It started as an applied research and development project, first to test the concept, which then led to the actual design and implementation of the operating system.

According to Microsoft, in 1995 Windows NT 3.x sales surpassed Unix to become the second largest supplier of network operating systems, with Novell Netware still holding the largest share. In 1996, Windows NT 3.x-4.0 outsold Netware to become the number one server operating environment. By mid-May 1997, more than one million copies of Windows NT Server 4.0 had been sold since its August 1996 launch date. Furthermore, an International Data Corporation Report stated Microsoft shipped 1.56 million Windows NT 4.0 Server licenses in 1998, nearly 50 percent more than Novell Netware and twice as many as Unix. By the end of 1998 Windows NT held a firm grasp on the number one spot in network operating environments with a 36 percent market share, compared to Novell's 24 percent share and Unix's 17 percent share. [Ref. 25]

With the release of Windows 2000, Microsoft has followed through on its strategy of operating system consolidation and formed a new family of servers. The Windows 2000 Server Family is the next generation of Windows NT and consolidates many of the features of Windows 95/98 into its operating system. The three members of the Windows 2000 Server Family are:

- **Windows 2000 Server Standard Edition** - (Formerly named Windows NT Server 5.0) The mainstream business server which includes the multipurpose capabilities required for workgroups and departmental server functions.

- **Windows 2000 Advanced Server** - (Formerly Windows NT Server 4.0, Enterprise Edition) A more powerful mid-range server that includes the full features set of Windows 2000 and advanced scalability.

- **Windows 2000 Datacenter Server** - The most powerful and functional server operating system offered by Microsoft for large-scale enterprise solutions. [Ref. 2]

Though not a true member of the Windows 2000 Server Family, Windows 2000 Professional should be mentioned at this point. Windows 2000 Professional is Microsoft's mainstream desktop operating system for businesses of all sizes. It replaces Windows NT Workstation 4.0, and as part of Microsoft's strategy of one operating system on the market, will replace Windows 98 as well. Windows 2000 Professional will offer the easiest Windows-based environment yet, the highest level of security, state-of-the-art features for mobile users, and better performance.

B. PURPOSE

This thesis introduces the Windows 2000 Server Family and the technologies and features of the operating system. The purpose of this thesis is to examine:

- Microsoft's strategy to consolidate operating systems.
- The existing differences between the Windows 2000 Server Family editions.
- What methods are involved in deploying or migrating an existing network to Windows 2000.
- What security features are introduced in Windows 2000.

C. ORGANIZATION

Chapter II discusses the history of Microsoft and its strategy leading to the development of Windows 2000. Chapter III investigates the Windows 2000 Server Family editions, features and technologies introduced in the operating system. Chapter IV discusses the methods of preparing an existing network for the deployment or

migration to Windows 2000. Chapter V discusses network security issues and features introduced by Windows 2000. Chapter VI offers some concluding thoughts.

II. MICROSOFT HISTORY AND STRATEGY

To understand Microsoft's strategy of operating systems consolidation, a discussion of the history of Microsoft and the origins of Windows NT is in order. Microsoft began developing Windows NT in 1988, but NT origins go even further back into Microsoft's history of operating systems development.

A. MS-DOS AND LAN MANAGER

By the mid-1980s, the PC world was very near to outgrowing the functionality it had gained through the implementation and success of DOS (Microsoft's version was named MS-DOS, for Microsoft Disk OS). DOS was a simple program loader that, while an acceptable model for an operating system, had several distinct disadvantages:

- DOS unloaded itself from memory when an application was launched, thus making the operating system unavailable during this time.
- Inability to run more than one program at a time - The command-line program access prevented launching more than a single program. DOS also assumed it had access to all addressable memory, making it inefficient to run more than one program.
- Lack of standardized graphics - Microsoft offered little graphics support in DOS, thus vendors were left to design proprietary graphics programming interfaces specific to their own hardware.
- Inability to access more than 1 megabyte (MB) of system memory - The DOS addressing scheme made it physically impossible to use more than 1 MB of memory. DOS-based programs still run up against this barrier even in these days of advanced technologies. [Ref. 3]

In the mid-1980's, Microsoft was faced with the problem of replacing DOS. At the time, Microsoft's own Windows product was not a true operating system but simply a shell (much like DOS-Shell) that ran on top of DOS.

In 1985, Microsoft launched MS-Net, which was based on DOS 3.x. MS-Net was influenced by several early network products, notably IBM PC Network and the 3Com 3+ program. Though decidedly slower and less reliable than Novell Netware, Microsoft launched MS-Net as the future to network solutions. LAN Manager was launched in 1987, and along with 3Com's 3+ Open LAN Manager and IBM's LAN server, was based on IBM's OS/2 operating system. OS/2 had most of the features required of an operating system of the time, including a Graphical User Interface (GUI), multitasking, and the ability to directly access up to 16 MB of memory. By 1991 several versions of LAN Manager began appearing at more-established companies, and were incorporated into several network operating systems, thus solidifying Microsoft's foothold in the networking industry. However, LAN Manager was not able to release Novell's powerful hold on the network market. Novell's Netware 3.x was released in 1987 and was tailored for Intel's 80386 processors, while LAN Manager remained based on Intel's 80286 processor. [Ref. 1]

B. WINDOWS AND WINDOWS NT

In late 1990, Microsoft and IBM parted company. Up to this point, Microsoft had focused much of its research and development into IBM's OS/2 systems. IBM had seen Windows as an intermediate step between DOS and Presentation Manager (IBM's name

for a Graphical User Interface (GUI) operating system). Microsoft put the word out to independent software developers that developing applications for Windows was the wave of the future.

As IBM and Microsoft cooperation broke down in the late-1980s, Microsoft began looking inward for software solutions. In 1987, Microsoft began developing Windows NT as a long-range follow-on to OS/2, and in 1988 formed what would later become the development team for Windows NT. Almost simultaneously, Windows 3.x and Windows for Workgroups 3.11 were in development. Though based on the 16-bit program model, these early versions of Windows provided standardized graphics, a GUI, the ability to perform several system functions, and a limited ability to run more than one program simultaneously. Windows 3.x offered Microsoft an operating system it could market for the desktop computers.

Around this time David Cutler, a Digital Equipment Corp. (DEC) veteran, joined Microsoft to design and build the next-generation operating system. Cutler had been one of the designers of the immensely popular VMS operating system for DEC's VAX machines. Cutler wanted to design Windows NT as a next-generation multiuser operating system and initially began by designing hardware built around Intel's i860 RISC chip. One of Cutler's conditions for moving to Microsoft was that he could bring around 20 former Digital employees with him, including several hardware engineers. Bill Gates readily met this demand - he knew hiring an OS architect of Cutler's stature was a coup,

and few engineers had Cutler's track record. In addition, Gates felt that Microsoft's long-term future depended on the development of a new OS that would rival UNIX.

After the dust had settled from Microsoft and IBM's breakup, Microsoft retained control of OS/2 3.0, dubbed Portable OS/2, which was in reality the basis for Cutler to build his NT project. Bill Gates soon realized that Cutler's design would extend beyond the desktop and was a step toward a server presence in the enterprise environment. [Ref. 4]

In 1993, after many delays, Microsoft released Windows NT 3.1 and Windows NT Advanced Server 3.1. Both operating systems broke new ground in terms of power, performance and reliability. Features included micro-kernel architecture, preemptive multitasking scheduler, x86/MIPS and Alpha support, domain server security, file and print services, and the NT File System (NTFS) [Ref. 5]. The development of Windows NT is shown in Figure 2.1.

Windows NT Advanced Server replaced Microsoft's OS/2 LAN Manager, though it was functionally almost identical to LAN Manager 2.2. Gates and Cutler had several philosophical disagreements during the initial phase of NT development, which was a primary cause for the release of Windows NT to be delayed. One such disagreement concerned the target microprocessor for Windows NT. Cutler originally wanted to design NT using a high-performance RISC processor while Gates felt he had to continue supporting the Intel processor family so applications would be readily portable between operating systems. Unfortunately, the i860 failed to function properly, causing further

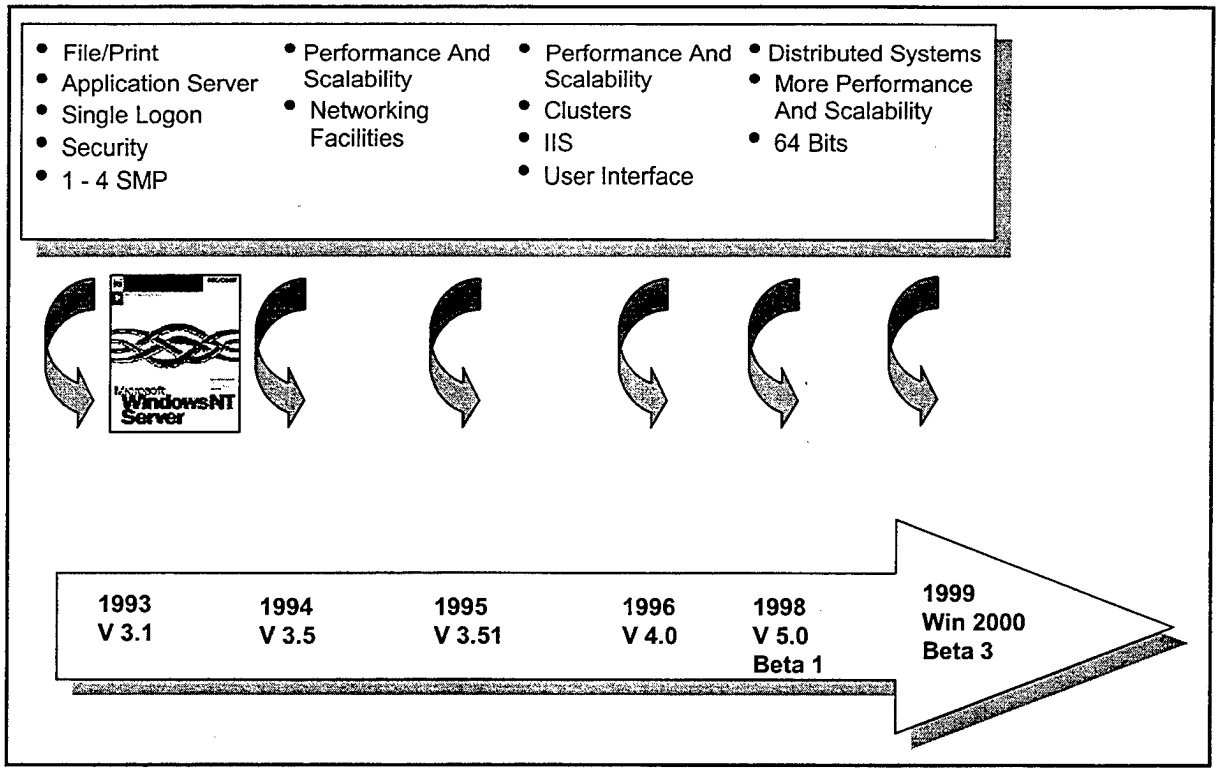


Figure 2.1. Microsoft Windows NT Server's development up to present. After Ref. [1]

problems when Microsoft decided to switch to the MIPS R4000 processor chip. Fortunately for Intel, hardware began catching up to the software. While development of Windows NT continued, Intel produced the 80486 processor, which was fast enough to run NT. While NT was not designed to be portable, it was designed to be ported, and the Intel and MIPS versions of Windows NT shipped at the same time. [Ref. 3]

The first release of Windows NT fell well short of expectations. Large corporation accounts were hesitant to invest in an untried network operating system from a company with a history of releasing early software versions riddled with bugs [Ref. 4]. Also, while Microsoft dominated the desktop PC market, it was in its infancy in the

networked enterprise arena. Well-entrenched competitors such as Novell, IBM, and Sun dominated the network market.

C. MICROSOFT'S STRATEGY OF A UNIVERSAL WINDOWS

Prior to the release of Windows 95 on September 5, 1995, Microsoft had released Windows 3.1, Windows for Workgroups 3.11, Windows NT Workstation 3.51, and Windows NT Server 3.51 operating systems. Windows 3.1 and Workgroup 3.11 were aimed at the small business and home users with a view to selling standard programs with a GUI on the PC platform. Windows NT was designed to handle applications on high-end workstations and servers. Microsoft discontinued the sale of Windows 3.1 and Windows for Workgroups 3.11 after the release of Windows 95.

Microsoft's strategy was clear -- A quick transition to Windows 95. Its aim was to remove all competition on the market for 32-bit operating systems for PCs, and to reduce support costs by providing a uniform operating system across its customer base. To accomplish this, Microsoft advertised Windows 95 as a user friendly operating system which contained a wider range of functions than previous Windows versions, offered full compatibility with legacy applications, and hardware requirements which were relatively inexpensive.

Microsoft's strategy owes its origins to Bill Gates' vision from 1987 of "Windows Everywhere" and his 1990 vision of "Information at your fingertips." That vision is based on a simple yet powerful idea: building computing systems that allow people to focus on information, rather than the technical aspects of the system that contains the information.

Microsoft wants to be the leader in all segments of the computer market. Their strategy was simple: PCs today, servers tomorrow, and in the future, everything that requires an operating system. Figure 2.2 illustrates Microsoft's timeline for operating systems consolidation.

Microsoft's strong position in the PC market will allow it to succeed in the low- and high-end computer market. Microsoft has designed a strategy to succeed in this endeavor by offering versions of Windows that are tailored to the low- and high-end markets, yet each will have the same look and feel of one Windows product.

Windows 95/98 and Windows NT 4.0 are an integral part of Microsoft's strategy of operating systems consolidation. Windows 95 established the Win32 API (Application User Interface) which is also resident in Windows NT. By September 1997, the sale of 32-bit applications in the U.S. amounted to 94 percent of the total sale of Windows applications. Over 100,000 applications were estimated to be compatible with Windows 95, of which more than 8,000 were compatible with Windows NT Workstation. [Ref. 1]

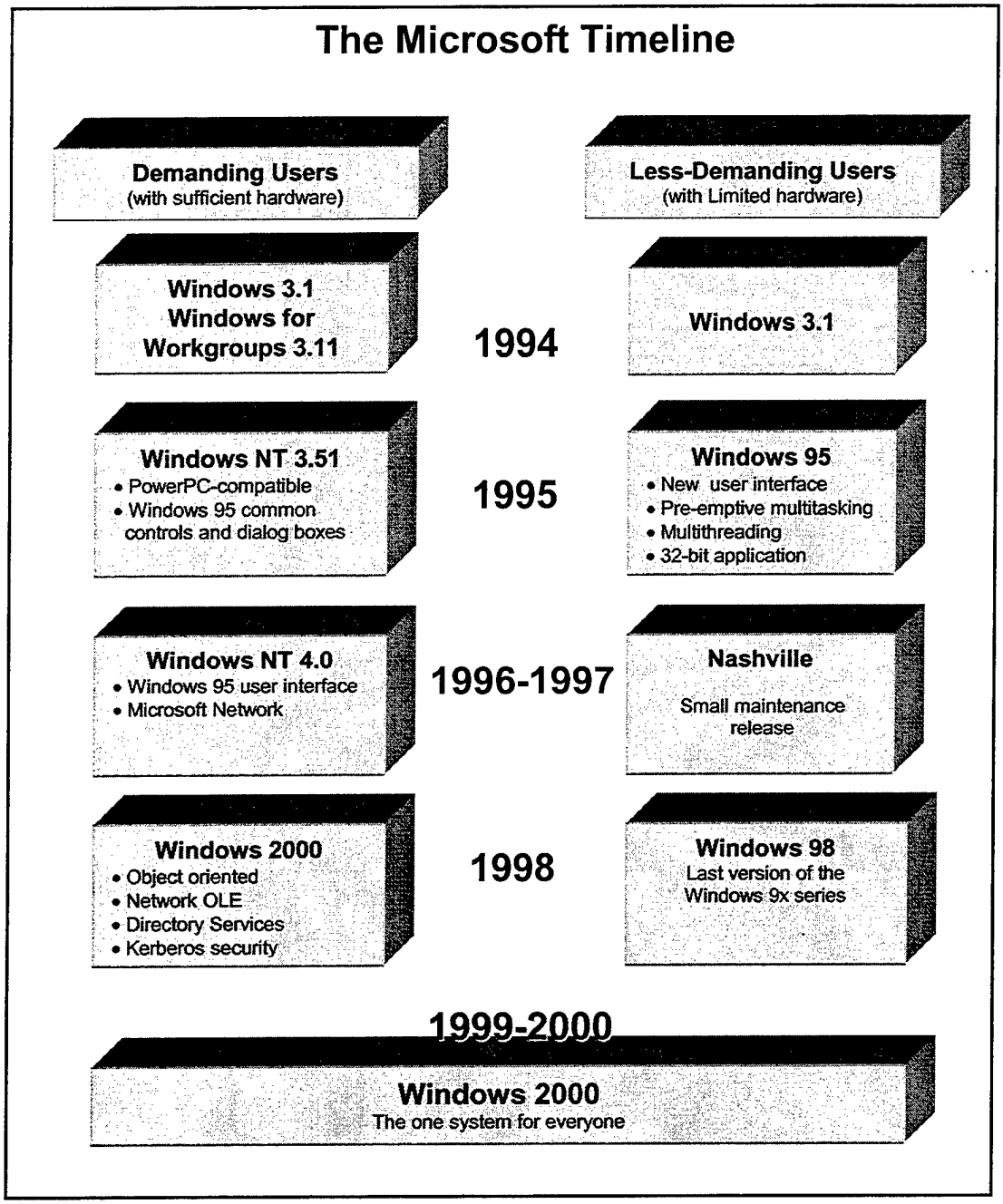


Figure 2.2. Microsoft strategy for operating systems consolidation. After Ref. [1]

1. Windows NT Workstation Leads the Way

Microsoft's strategy for the past few years has been for the Windows NT products to have the same "look and feel" of the Windows 9x technologies. This strategy has been successful with Windows NT Workstation in regards to the user interface and the APIs. While NT Workstation has not come near to reaching the popularity enjoyed by Windows 9x, this may be explained in part due to technology. NT Workstation has been, for the most part, ahead of end users, requiring larger RAM and faster processor chips, while being less compatible with older hardware and software.

As part of this strategy, Microsoft is emphasizing the advantages of the NT Workstation operating system over Windows 95/98:

- Better security facilities (such as NTFS)
- Greater integration with NT Server
- Improved use of Pentium processors
- Improved performance on computers with more than 16 MB RAM. [Ref. 1]

In addition to this strategy, Microsoft is moving forward with plans to establish itself in the high-end workstation market, currently dominated by Unix. Microsoft has gained momentum in this market as most of the important suppliers of workstation applications are now providing NT Workstation versions of their software. Another factor in favor of Microsoft is financial: A high-end PC and extra components are much less expensive than an identical Unix-based workstation. An entry-level system capable of running Windows NT can be purchased for less than $1,000, and even a mid-range

system capable of running server functions costs less than $2,000. Few, if any, Unix systems on the market cost less than $4,000, and server prices start at approximately $10,000. [Ref. 3]

2. Windows NT Server and Windows 2000

By mid-May 1997, more than 1 million copies of Windows NT Server 4.0 had been sold since its August 1996 release [Ref. 1]. Microsoft is now focusing on the high-end server market, where it has yet to gain a decisive piece of the market share. This market has been dominated by Unix-based servers, OS/400-based minicomputers (AS/400), MVS-based mainframes, and several other large operating systems. Microsoft's strategy for the future is to design a PC server that is scalable and able to handle any situation.

Scalability is the capability of a software or hardware product to grow almost unrestrained in processing throughput, provided the right technology is installed. With regard to operating systems, scalability means that it is possible to increase throughput; thus, if a server is extended from two to four processors, the throughput will almost double in the given applications. [Ref. 1] Windows 2000 will deliver scalability of up to 16 processors per server, an improvement of the market standard of four processors for most applications.

With the upcoming release of Windows 2000, Microsoft will push forward its strategy of "Windows everywhere" and will get Windows NT into the mainstream, spanning the entire computer market: home users, small businesses, to large multinational

corporations. Meanwhile, it will provide fixes and updates to its Windows operating systems. Windows 98 SE, Consumer Windows in 2000 (an extension of the Windows 9x line designed for the new hand-held PCs) and Consumer NT, are all being developed to fill the void left while waiting for the release of Windows 2000. Table 2.1 illustrates Windows operating systems anticipated development and release.

Windows Roadmap						
	1st half 1999	**2nd half 1999**	**1st half 2000**	**2nd half 2000**	**2001 to 2002**	**2003**
Windows NT	Windows NT 4.0 Service Pack 5	Win2000 Pro, Server, Advanced Server, Windows NT Embedded 4.0	Win2000 Datacenter; *Win2000 Service Pack 1	*Win2000 Small Business Server; *64-bit Win2000	Consumer Windows NT (code-named Neptune)	*Successor to Win2000 Pro and Server versions expected
Windows 9X	Internet Explorer 5	Windows 98 Second Edition with Service Pack 1		Consumer Windows in 2000 (code-named Millennium)	No more significant upgrades to the 9x line?	
Windows CE		*Win CE 3.0 (Code-named Rapier)				
Estimated time frame						

Table 2.1. Roadmap of Windows software development. From Ref. [6]

D. CHAPTER SUMMARY

Microsoft's Windows NT Server and Workstation have quickly become the operating system of choice for large and small enterprises. The Gartner Group reports that by the year 2000, 50 percent of all enterprises will be using the Windows NT Server

operating system, and that number could increase to 90 percent by 2003 [Ref. 7]. First designed as a specialized operating system for technical and business needs, Windows NT will make the transition to a mainstream product for businesses on both the client and server. The immense popularity of Windows NT ensures that the evolution of Windows 2000 is welcome and inevitable, and with the new features, desirable across the entire market.

III. WINDOWS 2000 SERVER EDITIONS AND FEATURES

The Windows 2000 Server operating systems are Microsoft's vehicle to carry them into the new millennium. The Windows 2000 Server family offers scalability and advanced directory technology to network administrators. Windows 2000 builds on the strengths of Windows NT 4.0 by delivering increased reliability, availability, and scalability with end-to-end management features that are designed to reduce running expenses, or the total cost of ownership (TCO). Microsoft's initiatives to reduce TCO include a group of applications called *Zero Administration for Windows (ZAW)*. ZAW is a collection of several different technologies with the goal of establishing an effective infrastructure for management. [Ref. 8] This chapter discusses the Windows 2000 Server editions and the server-side technologies included in the operating systems. Some technologies and features are discussed within the context of the Windows 2000 Server edition in which it is introduced (such as Microsoft Cluster Server), while other features that span the entire Windows 2000 Server family (such as Active Directory) are discussed separately.

A. WINDOWS 2000 SERVER EDITIONS

The Windows 2000 Server family consists of three editions: Standard, Advanced, and Datacenter. Table 3.1 lists the different server versions and a quick description of features. The Standard edition is expected to be the most popular version for small to

medium-sized businesses, while the Advanced and Datacenter editions are designed to meet the needs of mission critical deployments in medium, large, and Internet Service Provider (ISP) organizations. [Ref. 2]

Windows 2000 Server Family

Product	Description	Features
Windows 2000 Server Standard Edition	The mainstream business server includes the multipurpose capabilities required for workgroups and departmental deployments of file and print servers, application servers, web servers, and communication servers.	Active Directory Windows Management Tools Kerberos and Public Key Infrastructure (PKI) Security Windows Terminal Services COM+ component services Enhanced Internet and Web Services Up to 2-way SMP support (existing users will get 4-way SMP)
Windows 2000 Advanced Server	A more powerful mid-range server that includes the full features set of Windows 2000 Server and adds the advanced high-availability and improved scalability required for enterprise and larger departmental solutions.	All Windows 2000 Server features Network load balancing Enhanced Application failover clustering Component Load balancing High-performance sort Up to 64 GB main memory Up to 4-way SMP (existing users will get 8-way SMP)
Windows 2000 Datacenter Server	The most powerful and functional server operating system ever offered by Microsoft for large-scale enterprise solutions.	All Windows 2000 Advanced Server features Up to 16-way SMP (32-way through OEMs) More Advanced Clustering

Table 3.1. The Windows 2000 Server Editions and Features. From Ref. [2]

1. Windows 2000 Server Standard Edition

Windows 2000 Server is the follow-on operating system to the popular Windows NT 4.0. Originally named Windows NT 5.0, this edition is a multipurpose operating system that builds on the strengths of Windows NT 4.0 by providing a platform that is faster, more reliable, and easier to manage. It delivers a comprehensive set of distributed infrastructure services based on the Active Directory (discussed later in this chapter) directory service. Although Windows 2000 Server offers significant new functionality, it is designed for modular deployment to allow end-users to take advantage of new features and technologies at a pace best suited for their organization. [Ref. 9]

Windows 2000 Server provides a comprehensive set of web and Internet services that allow organizations to take advantage of the latest Web technologies. It provides an integrated, flexible web platform with the full range of services businesses require to deploy intranets and critical Web-based business solutions.

Hardware requirements for operating systems are difficult to specify because hardware improves at an ever increasing pace and user needs and expectations change accordingly. Microsoft provides the following minimum system requirements for the Windows 2000 operating systems:

- 166 MHz or higher Pentium-compatible microprocessor or Alpha CPU
- 32 MB RAM for Windows 2000 Professional; 64 MB RAM for Windows 2000 Server
- 2-GB hard disk with a minimum of 500 MB of free space

- VGA monitor and video card
- Keyboard and mouse
- A network card or CD-ROM to retrieve the setup files. [Ref. 8]

Note that these are the *minimum* hardware requirements for running Windows 2000 Server. A system with at least a 300 MHz Pentium II (or equivalent) with 128 MB RAM for Professional and 256 MB RAM for Server would provide for adequate-to-optimum performance. Some network professionals even recommend the addition of dual processors [Ref. 10].

2. Windows 2000 Advanced Server

Windows 2000 Advance Server, formerly Windows NT 5.0 Enterprise Edition, contains all the features and functionality of Windows 2000 Server Standard Edition, plus many additional features for businesses and organizations that require higher levels of scalability, reliability, and availability. Integrated system scalability is provided through enhanced symmetric multiprocessing (SMP). In addition, Advanced Server provides three multi-node technologies: Clustering, TCP/IP load balancing, and application component load balancing.

a. Symmetric Multiprocessing (SMP)

SMP allows software to use multiple processors on a single server in order to improve performance. SMP makes demands on the server's capability to provide the necessary bandwidth for the given number of processors and on its efficiency in sharing

task among the processors. It also makes great demands on the capability of the overall operating system to divide the tasks into small, independent parts, so that the numerous processes being executed on the processors are not temporarily suspended [Ref. 1]. Advanced Server supports up to 4-way SMP, and improvements in the implementation of SMP code allow for improved linearity, making Advanced Server an even more powerful platform for business-critical applications. Existing Windows NT. 4.0, Enterprise Edition servers with up to 8-way SMP can install enhanced SMP [Ref. 11].

b. Clustering

Windows 2000 Advanced Server provides clustering system services as a standard feature with Microsoft Cluster Server (MSCS). Clustering is the act of combining multiple systems (or servers) to act as a single, redundant system, and provides high levels of availability through redundant CPUs, storage and data paths. The cluster configuration is managed as if it were a single server. With clustering, when one server fails, a second server can automatically pick up the failed server's workload in less than a minute, in a process known as fail-over. The monitoring services will detect the failure and shift responsibility to the designated backup server, reconnect clients and migrate shared storage and file shares. A more detailed discussion of clustering is offered later in this chapter. [Ref. 8].

c. TCP/IP Network Load Balancing

Similar to clustering, Network Load Balancing (NLB) enables organizations to cluster up to 32 servers running Windows 2000 Advanced Server to evenly distribute incoming traffic, providing a single image to the client. In today's booming growth of the Internet and intranets, Web servers are increasingly serving as the front-end to multi-tiered networks. NLB allows mission-critical servers, through which Web-based applications connect, scale their performance to match the demand. NLB will automatically reconfigure the cluster to direct requests to other servers when a computer fails or goes offline for maintenance, providing continuous availability of network services. Network Load Balancing benefits include:

- Scalable performance
- Load-balances requests for individual TCP/IP services across the cluster.
- Supports up to 32 servers in a single cluster.
- High availability.
- Automatically detects and recovers from a failed or offline computer.
- Automatically redistributes the network load when the cluster set changes.
- Recovers and redistributes the workload within 10 seconds.
- Handles inadvertent subnetting and rejoining of the cluster network.
- Controllability
- Integrated with the networking infrastructure of Windows 2000 Advanced Server.

- Requires no specialized hardware.
- Lets clients access the cluster with a single Internet logical name and IP address, while retaining individual names for each computer.
- Server applications need not be modified to run in a NLB cluster.
- Computers can be taken offline for preventive maintenance without disturbing cluster operations. [Ref. 11]

d. Component Load Balancing

Windows 2000 Advanced Server offers a third multi-node technology for use in a three-tier architecture (application layer, data server, and user interface layers) called Component Load Balancing. Component Load Balancing is ideal for use in the application tier, enabling the creation of up to 8-node application server clusters for high levels of application availability.

When the Component Load Balancing Server receives a request, it routes the request to the appropriate application server based on server load. In the case of a server failure, the Component Load Balancing server is notified and routes requests away from the failed node. [Ref. 14]

3. Windows 2000 Datacenter Server

Windows 2000 Datacenter Server is the most powerful and functional server operating system ever offered by Microsoft. It supports up to 16 SMP or 32 SMP through original equipment manufacturers (OEM), and up to 64 GB of physical memory.

Windows 2000 Datacenter Server includes all the features of Windows 2000 Advanced Server but is optimal for:

- Large data warehouses
- Econometric analysis
- Large-scale simulations in science and engineering
- Online transaction processing
- Server consolidation projects
- Large-scale ISPs and Web site hosting. [Ref. 11]

Windows 2000 Datacenter Server promises Microsoft's best scalability and clustering capabilities, as well as Microsoft's venture into providing an operating system offering mainframe features. Features include 4-way clustering (Advanced Server offers 2-way) and mainframe-like administration tools such as Job Object, which allow system managers to assign resources to a particular task. Microsoft recently demonstrated a Compaq Alpha server running a 64-bit version of Datacenter Sever and a 64-bit version of SQL Server (not yet released). This scenario enabled the system to support up to 8 terabytes of memory. [Ref. 15]

Windows 2000 Datacenter Server's potential scalability promises two major benefits: the ability to host large enterprise applications' particularly databases; and the possibility of consolidating many small, single-application NT servers into one large server, decreasing administration and management problems.

B. WINDOWS 2000 FEATURES

Windows 2000 is not merely an upgrade from Windows NT 4.0, but a new innovation of technologies and management tools. In this section several of the most important and useful features and management devices will be introduced. These are the Active Directory, which allows administrators to track and locate any object on a network, the Microsoft Management Console, which is a framework for administrative tools, the Microsoft Cluster Service, which provides for the combining of multiple systems to act as a single, redundant system, and the Distributed File System, which allows file shares to be maintained redundantly between multiple servers.

1. Active Directory

With the tremendous growth in network computing, the need for a powerful, tightly integrated directory service has become increasingly important. Windows NT Server 4.0 offers the Windows NT Directory Services, a robust directory that delivers a single network logon and a single point of administration and replication. Active Directory is Microsoft's new directory service to help manage a network in today's global networking environment. It is Microsoft's first enterprise-class directory that is scalable, designed to take advantage of Internet technologies, and fully integrated at the operating system level. Active Directory supports a wide range of well-defined protocols and formats and provides powerful, flexible, and easy to use APIs. Possibly the greatest

service Active Directory provides is to administrators and users with a "one-stop shopping" source for resource and management information.

a. Directory Services

A directory service is a physically distributed, logically centralized storage place for data that is used to administer the entire networking environment. Traditionally, directory services have been tools for organizing, managing, and locating objects in a computing system. Objects are elements - printers, documents, e-mail addresses, databases, users, distributed components, and other resources - that users and applications require to perform their jobs and functions.

Directory services perform functions similar to a telephone book. A white-pages-type search is based on specific input (a person's name, for example) in which a specific output is received. A yellow-pages-type search is based on general input (a type of printer or location of printers, for example) in which a listing of resources is received. [Ref. 3]

b. Active Directory Overview

As LANs and WANs grow larger and more complex, connect to the Internet, and applications demand more from the network, more is required from a directory service. Microsoft's Active Directory was created to meet the challenge of unifying and bringing order to diverse server hierarchies, or namespaces. A namespace is

a type of directory. When used in the context of networking, Active Directory provides a namespace for resolving the names of network objects to the objects themselves [Ref. 8].

Active Directory will fulfill a wide variety of naming, query, administrative, registration, and resolution needs, in addition to the traditional administrative tasks. Figure 3.1 illustrates the overall functions Active Directory will provide in an enterprise system.

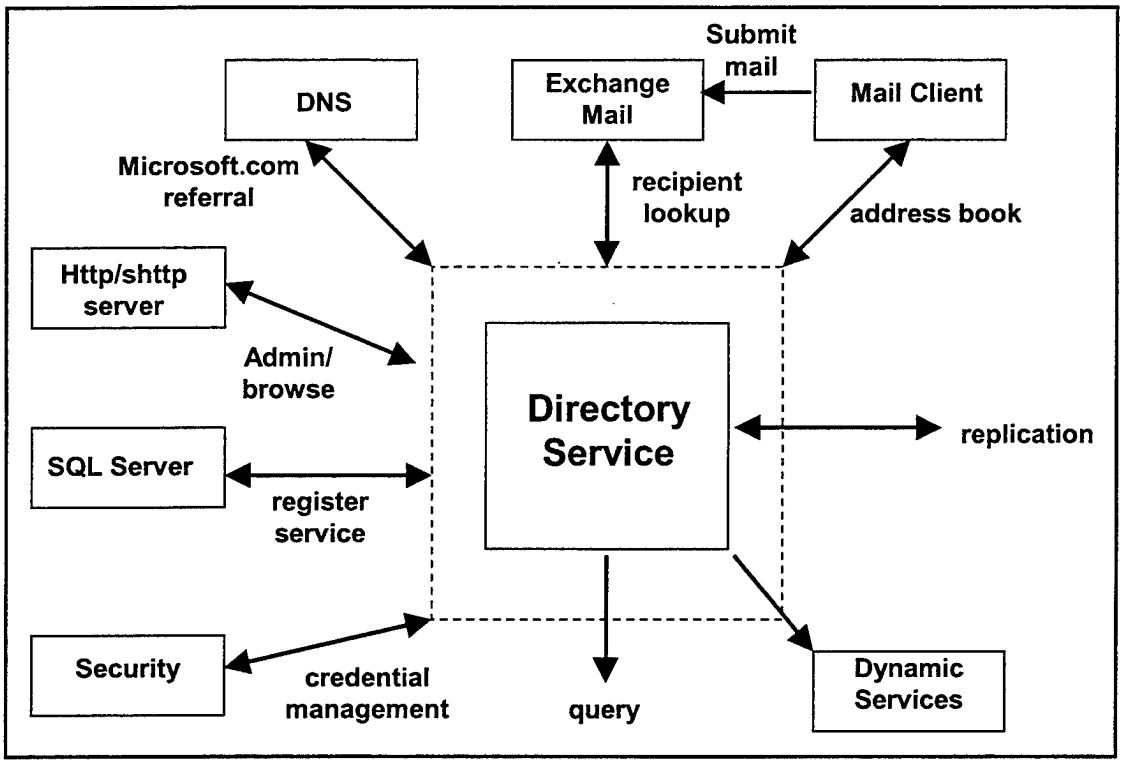


Figure 3.1. Active Directory is a service provider used to locate all network services and information. From Ref. [16]

Windows NT included many separate services to help administrators and users find network resources. Network Neighborhood proved to be useful but often

clumsy and unpredictable. WINS Manager and Server Manager could be used to list network resources (objects) but was unavailable to end users. Finally, administrators used User Manager to manage user accounts (another type of network object), but this tool also proved to be inefficient, especially in large networks.

All of these objects reside in a common container: the Microsoft Windows NT domain. A Windows NT domain is an group of client and server computers referenced by a specific name that share a single security permission database. Currently, administrators of large environments are forced to partition their network into multiple domains interconnected with trusts. Active Directory is introduced in Windows 2000 to replace domain functionality. Active Directory can be replicated between multiple domains, so that no single system is critical, making Active Directory both redundant and load-balanced. [Ref. 8]

Active Directory includes the following features and benefits:

- Support for open standards to facilitate cross-platform directory services, including support for the Domain Name System (DNS), and support for standard protocols, such as LDAP (Lightweight Directory Access Protocol).
- Support for standard name formats to ensure ease of migration and ease of use.
- A rich set of APIs, which are easy to use for both the scripter and C/C++ programmer.
- Simple, intuitive administration through a simple hierarchical domain structure and the use of drag and drop administration.
- Directory object extensibility via an extensible schema.
- Fast lookup via the global catalog.

- Speedy, convenient updates through multimaster replication.
- Backward compatibility with previous versions of the Windows NT operating system.
- Interoperability with Netware environments. [Ref. 3]

c. Single-Point Administration

Active Directory allows a single point of administration for all published resources, which can include users, files, devices, host connections, databases, Web access, and services. Active Directory makes use of Domain Name System (DNS) as its locator service, organizes objects in domains into a hierarchy of organizational units (OUs), and allows multiple domains to be connected into a tree structure. Perhaps the best feature for domain administrators is the use of domain controllers instead of primary and backup domain controllers.

d. Active Directory Concepts

Active Directory redefines the NT domain structure and how domains interact. Active Directory is a completely new three-dimensional, hierarchical solution to directory services. The four concepts of Active Directory are the following:

- ***Domain*** - The fundamental grouping of Active Directory. The domain contains the numerous objects that can be structured through OUs. At its foundation, the domain corresponds to the X.500 directory structure specifications, but the domain is not described in the same way, because X.500 does not allow for the establishment of a hierarchy of organizations.
- ***Organizational Unit (OU)*** - Enables each domain to be split into a number of more manageable units, based on a hierarchical structure, making Active Directory a three-dimensional solution.

- ***Groups*** - Collections of objects of the same type as used in Windows NT 4.0 domains.

- ***Objects*** - Objects can be a user or a resource, as in NT 4.0 domains. A container is a special type of object used to organize Active Directory. Containers are used to group other objects and can be nested within other containers. [Ref. 1]

Another concept important to understanding Active Directory and the replication process is the use of *sites*. A site is a collection of well-connected machines with high bandwidth connectivity and based on IP subnets. To configure a site object in Active Directory, you associate it with one or more TCP/IP subnets. A site is a geographically determined boundary, separate from domain boundaries. For example, a site may span multiple domains and a domain may span multiple sites. Sites are not part of the domain namespace but control replication and help determine resource locations.

Everything Active Directory tracks are considered objects and each object is defined by attributes. Attributes describe objects in Active Directory. For example, User objects share attributes to store a user name, full name, and description. System objects share a separate set of attributes, such as host name, IP address, and physical location.

The set of attributes available for each particular object type is called a schema. The schema makes object classes different from each other. This information is actually stored within Active Directory, which allows administrators to add attributes to

object classes and have them distributed across the network to all domains, without restarting any domain controllers.

Each object in an Active Directory has a name, identified as a Lightweight Directory Access Protocol (LDAP) distinguished name. LDAP distinguished names allow any object within a directory to be identified uniquely regardless of its type, and are discussed later in this chapter.

A set of objects within Active Directory is described as a *Tree*, while *Forest* describes trees that are not part of the same namespace but share a common schema, configuration, and Global Catalog. Global Catalog is a service within Windows 2000 that allows users to find any objects to which they have access. [Ref. 8]

e. Active Directory Trust Relationships

Domains remain a part of Active Directory but domain trusts are completely redefined. Active Directory removes the worst drawbacks of current trust relations. In Windows NT 4.0, trusts could be one-way or two-way. In Active Directory, all trusts are two-way, or bi-directional. More importantly, all trusts are transitive, which means that a trust exists between two domains if both have trust relationship with a common intermediate domain. For example, if Domain A trusts Domain B, and Domain B trust Domain C, then there is an automatic implicit trust between Domain A and Domain C. The introduction of transitive trusts reduces the number of trusts necessary to create a full trust from $N(N\text{-}1)$ to N -1, where N is the number of domains. This will

dramatically simplify administration of large networks using multiple domains. Figure 3.2 illustrates the use of transitive trust relationships.

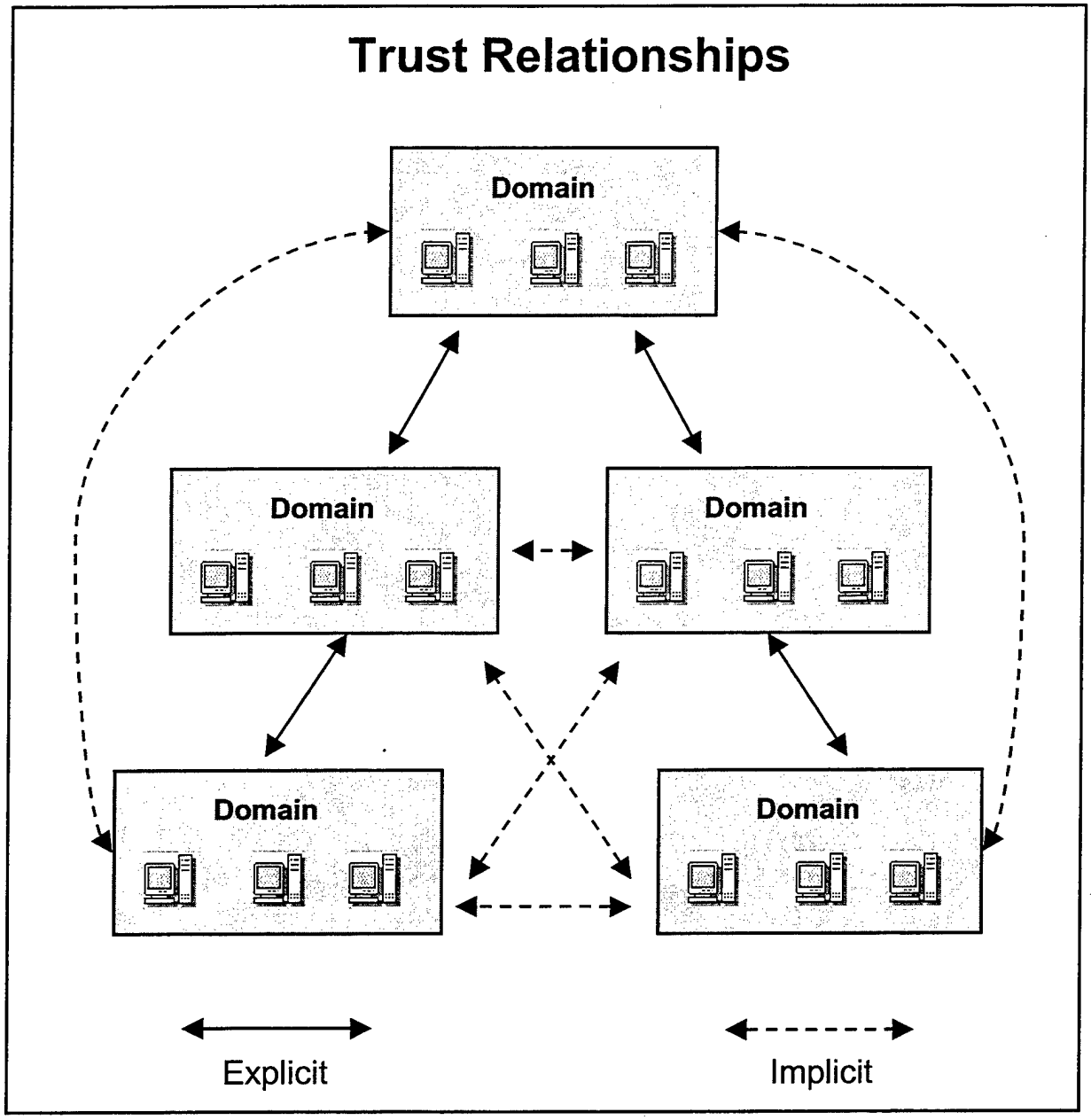


Figure 3.2. Trust Relationships with Windows 2000 and Active Directory. After Ref. [1]

f. Partitioning and Replication

Large networks will most likely contain hundreds of thousands of objects. Windows NT 4.0 required multiple domains to allow that large of number of objects to be manageable. With administrators limited to a 40 MB database, they were forced to divide users and resources into domains and create trusts between the domains.

Active Directories can be partitioned to lesson the load on domain controllers. Partitioning allows different domain controllers to manage different sections of the database, reducing the load on any individual server. Clients can use resources located within different Active Directory partitions transparently. This enables administrators to manage massive Active Directory domains without requiring domain controllers to handle the entire database. Also, Active Directory allows multiple tree directories, one for each domain [Ref. 8].

Another innovation in Windows 2000 architecture involves replication and fault tolerance. Windows 2000 eliminates the primary domain controllers (PDCs) and backup domain controllers (BDCs) in favor of domain controllers (DCs). PDCs are a single point of failure in NT 4.0 and may be a source of performance problems for large WANs. In an Active Directory, all DCs are completely equal to each other.

The conversion to DCs is a result of Active Directory's introduction of multimaster replication, which enables changes to be made to a domain on any Windows 2000 server that contains a writeable copy of the domain database. Each server keeps track of which updates it has received from which servers, and can intelligently request

only necessary updates in case of failure. Multimaster replication also allows updates to the domain databases of the servers in the manner best suited for WAN lines. [Ref. 16]

g. DNS (Domain Name System) Support

DNS is necessary to any Internet-connected organization. DNS provides name resolution between common names (MyName.MyCom.com) and the IP addresses that network layer components use to communicate. Active Directory makes extensive use of DNS technology and relies on DNS to locate objects within Active Directory. In fact, in Active Directory, domain names are DNS names. In contrast, Windows NT 4.0 required NetBIOS names to be resolved to IP addresses, and to rely on WINS or other NetBIOS resolution techniques [Ref. 8].

h. Global Catalog

Global Catalog is a service within Windows 2000 Server that allows users to find any objects to which they have been granted access, regardless of which domain it is placed in, by searching for certain specific properties. It is designed to handle queries on objects throughout the entire domain tree, quickly and efficiently. This is possible because Global Catalog contains information on objects from all domains in the domain tree, therefore, a query on an object from another domain is carried out promptly and with minimal help from other domain controllers.

It is important to note that Global Catalog is an index stored on Active Directory servers. It contains the names of all objects in the Active Directory server,

regardless of how the server has peen partitioned. Specifically, Global Catalog does not contain a full replica of all objects in the directory - it contains an entry for all objects but not all the attributes. Users are limited to a handful of searchable attributes for each object, such as the distinguished names, first and last names of users, and printer names or locations. Administrators are given the ability to specify other attributes that users tend to search on, by using the Active Directory Schema.

i. LDAP and ADSI

The Lightweight Directory Access Protocol (LDAP) is an Internet Proposed Standard (RFC2251) for accessing directory services, and reflects Microsoft's trend toward relying on standard protocols. LDAP defines how clients and servers exchange information about a directory. Of note, Active Directory is not an X.500 directory. Rather, it uses LDAP as the access protocol and supports the X.500 information model without requiring systems to host the entire X.500 overhead [Ref. 3].

Microsoft developed Active Directory Services Interface (ADSI) as a means to write directory-enabled applications that access Active Directory and other LDAP-enabled directories. ADSI is a set of extensible, easy-to-use programming interfaces that can be used to write applications to access and manage:

- Active Directory
- Any LDAP-based directory
- Other Directory Services in a customer's network, including NDS. [Ref. 16]

Network administrators will use ADSI to automate common administrative tasks, such as managing users and groups, printers, and setting permissions on network resources.

In summary, the addition of Active Directory is, by itself, a strong argument to update or migrate to Windows 2000 Server. Active Directory combines Windows NT domains with Internet domains and makes them scalable to enterprise proportions. It will provide users with dynamic search capabilities while easing administrative and management loads on the network. While Active Directory may certainly start off having the greatest impact in large organizations with complex IT infrastructures, Active Directory still offers enhancements to small and medium-sized businesses and organizations, through enhanced security, replication, and administration.

2. Microsoft Management Console (MMC)

Microsoft Management Console (MMC) is a windows-based frame system designed to show multiple documents loaded with administrative information. MMC does not provide any management behavior, but provides a common environment that acts as a host system for all administrative tools called S*nap-ins*. Snap-ins will provide the actual management behavior. Administrators will be able create tools from various Snap-ins and then save these tools for later use. MMC can run on Windows 95/98, Windows NT 4.0, and Windows 2000 operating systems [Ref. 17].

a. MMC Overview

MMC is an effort by Microsoft to create better tools to administer Windows operating systems. The Microsoft Windows administration development team defined a common host for many of its own tools. The MMC project's initial goal was to support simplified administration through integration, delegation, task orientation, and overall interface simplification. As Microsoft addressed that goal, it increased the project's scope to include all Microsoft administration tools, and to offer MMC as a generalized framework to its many independent software vendors (ISVs). [Ref. 17]

As mentioned above, MMC does not contain any management facilities, but provides a common environment for Snap-ins. Snap-in software constitutes the smallest unit in the console, or window that handles the MMC software, and contains some management functions. Snap-ins are purely technical OLE (Object Linking and Embedding) server processes or applications, and can function independently of one another or act as extensions of functionality in other Snap-ins [Ref. 1]. A standalone Snap-in provides functionality even while acting independent of other Snap-ins. An extension Snap-in provides functionality only when it is called by another Snap-in.

The next level in MMC is the *console*, which provides the graphical display of the management software. The console can contain more than one Snap-in, which can be saved in a Management Saved Console (MSC) file. An administrator can later open or send the MSC file to other administrators, who can open the file and immediately have a recreation of the customized Snap-in. Several MMC consoles may be

handled simultaneously on the same computer, but each console requires its own copy of MMC. [Ref. 1]

b. The MMC User Interface

The MMC is a Windows-based Multiple Document Interface (MDI), which allows more than one frame to be open simultaneously, enabling the administrator to view one or more Snap-ins containing the actual management tool. As seen in Figure 3.3, the MMC User Interface (UI) is very similar to Windows Explorer. The MMC UI normally consists of a parent frame and children's windows.

The components of the Microsoft Management Console User interface (illustrated in Figure 3.3) are as follows:

- ***Scope pane.*** The scope pane is the left window in MMC and lists all of the services that can be administered through MMC. This hierarchy of services is also called the namespace. This may include multiple servers and multiple services, such as Microsoft Transaction Server (MTS) and FTP Server.

- ***Results pane.*** The right window in MMC. When you select a node in the scope pane, the Results pane displays a list of all elements and services that fall within the selected node's domain.

- ***Rebar.*** In addition to the two window panes, MMC has three menu bars, the lowest of which is the Rebar. The Rebar consists of **Action** and **View** menus, plus two additional toolbars, or bands. The commands associated with Rebar menus and bands all change with respect to the selected node. Functions tied to individual services, such as Performance Monitor for Internet Information Server, are all found on the Rebar.

- ***Nodes.*** Nodes, which appear in the tree view of the scope pane, are instances of individual services. For example, a computer on a network or a Web service on a particular (hardware) server may appear as a node in the scope pane of MMC. You can open the property sheets of any node by right-clicking it and then selecting **Properties** on the shortcut menu. [Ref. 18]

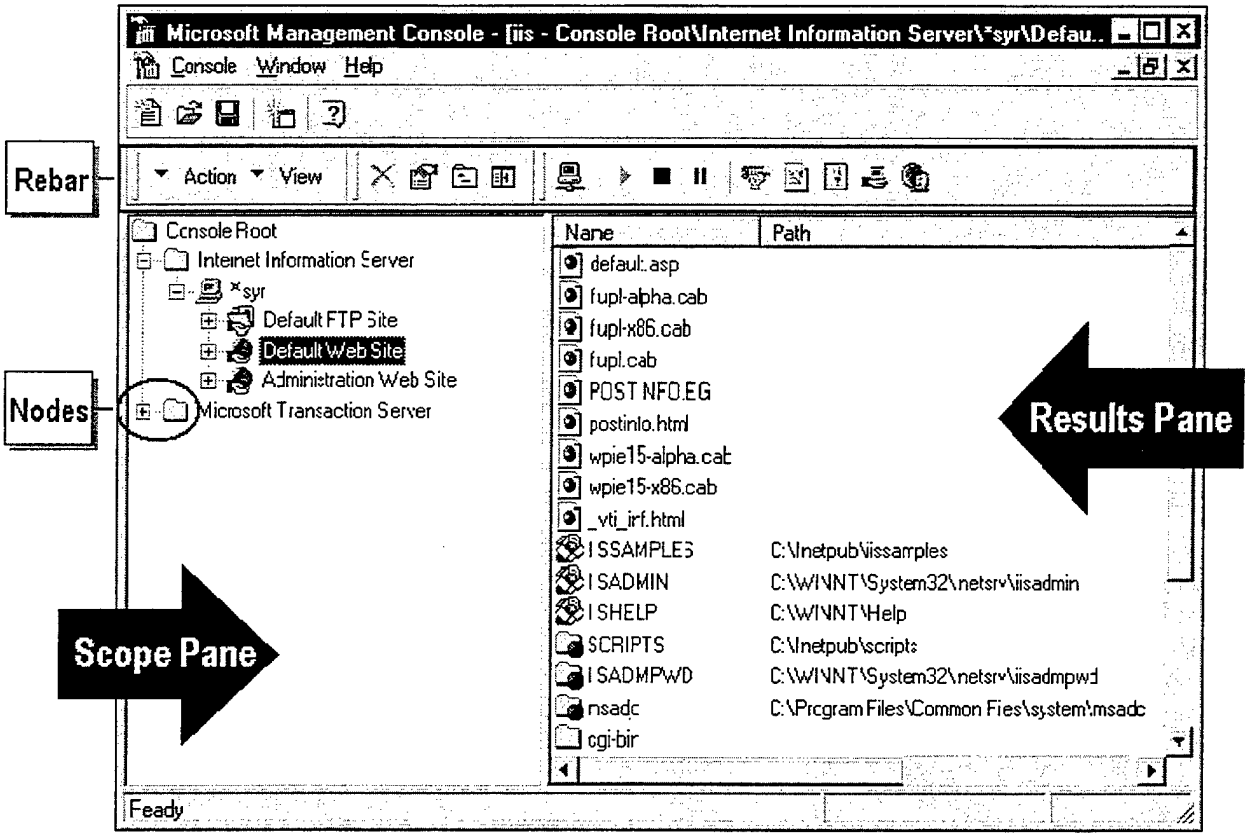


Figure 3.3. The Microsoft Management Console. From Ref. [18]

The MMC can also be designed to offer a scaled-down view, such as a simple task-oriented taskpad as seen in Figure 3.4, or by condensing the view to a single tool, as seen in Figure 3.5.

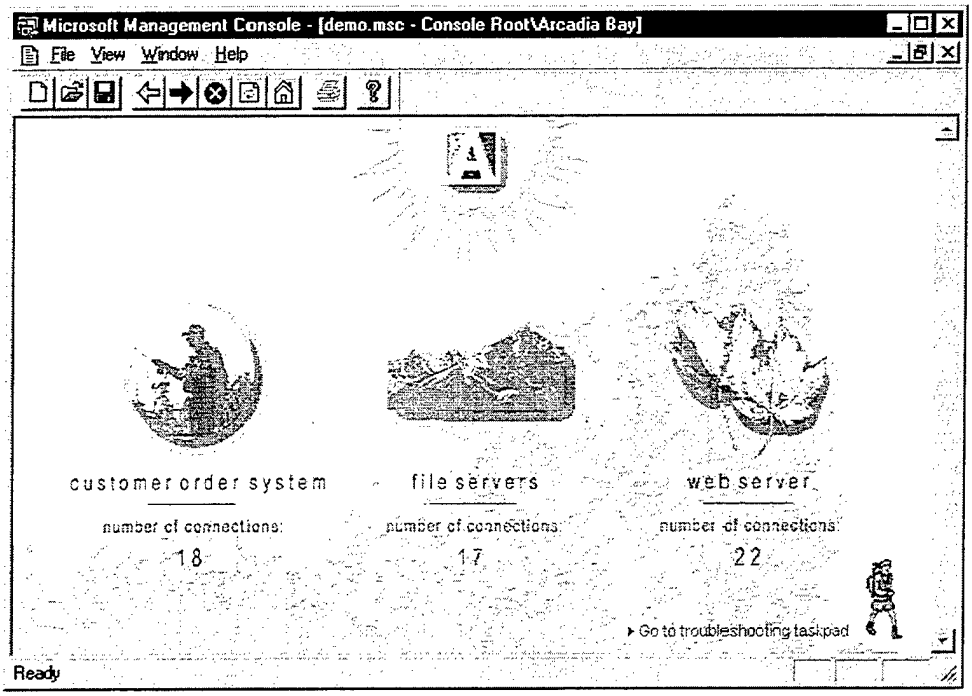


Figure 3-4: Simplified view of the MMC. [Ref. 17]

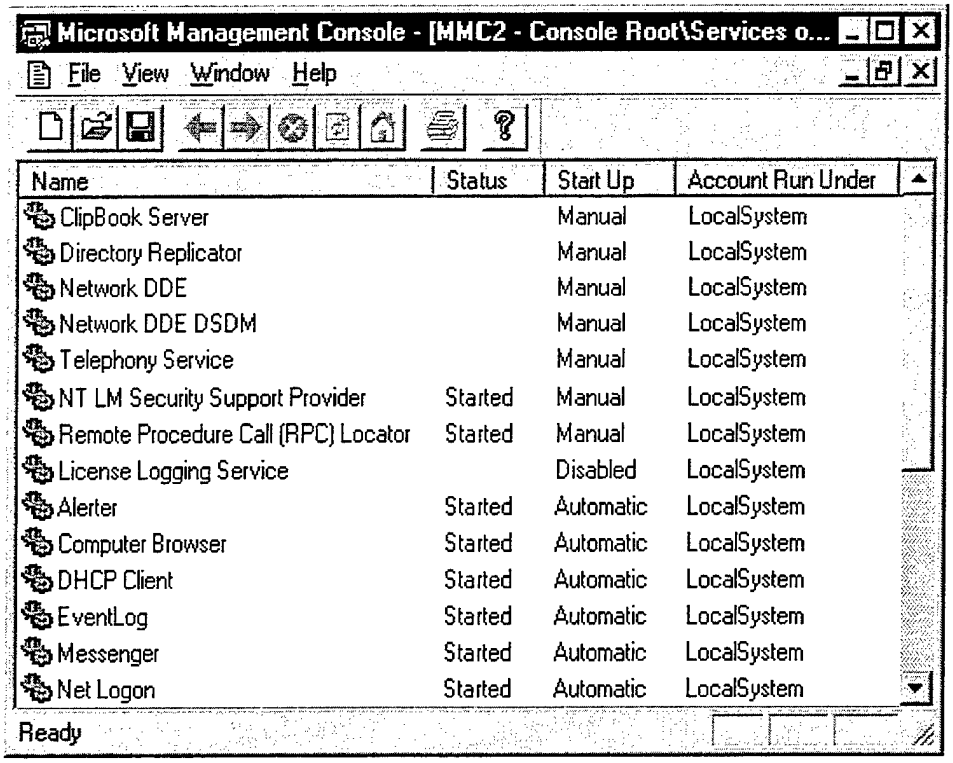


Figure 3-5: MMC viewed as a single tool, such as a service management windows. [Ref. 17]

The MMC console is heavily influenced by the latest Internet technologies. Remember that the console itself has no management behavior; it is a host that contains other Snap-ins - which is literally software - that extend the console to offer the actual management capabilities. The UI elements of the tool interact with the MMC Snap-in Manager, which interacts with the various Snap-ins. The Snap-in Manager also deals with saving settings into the MSC file. Figure 3.6 depicts how this works.

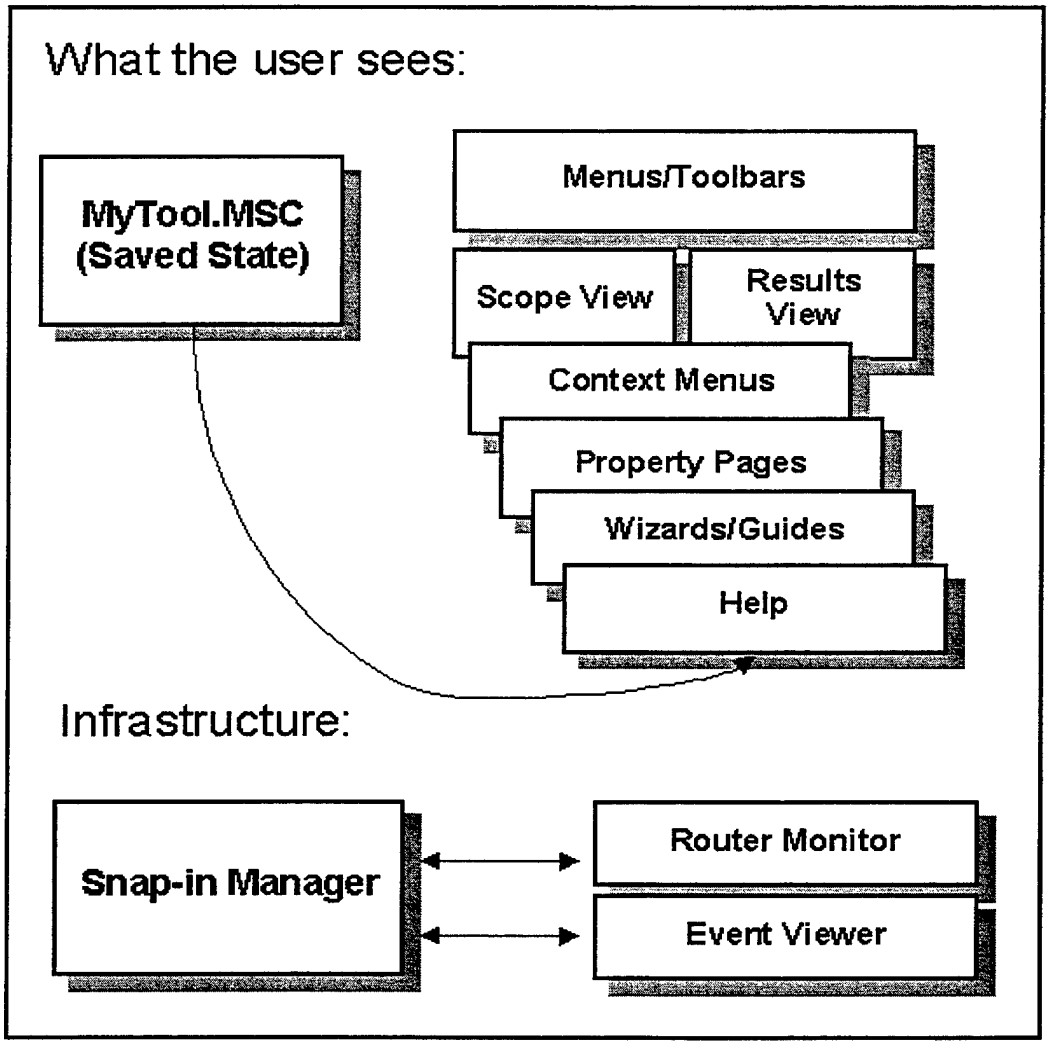


Figure 3.6. The MMC Model. After Ref. [17]

When an MMC console is activated, one or more Snap-ins are initialized. These Snap-ins jointly make up the namespace of the console, which are the collection of elements that appear in the scope pane. The namespace is the master tree, defining what tasks the console is capable of performing. Other panes in the MMC console are just different displays of the namespace; every display can have its root in a different part of the tree, yet all point to the same fundamental data source, which ensures consistency of the console environment. [Ref. 1]

c. Benefits of using MMC

MMC is a full management solution, provided the administrator takes full advantage of the necessary MMC Snap-ins. MMC provides several key benefits, including:

- **Task Orientation.** The tools being defined to work with MMC are task oriented in nature- they cater to the task being performed rather than merely displaying the raw objects that can be manipulated. Administrators can also create and customize their own tools that contain only the UI they need to complete the tasks.

- **Integration.** The UI for all the management tasks an administrator must perform are collected into a single console. As upgrades or new applications are added to the network, their administration is integrated into the existing administration common console.

- **Delegation.** Administrators can easily modify existing tools to create new tools that can then be given to other users. An administer could modify a tool with reduced functionality and less complex views of the tool namespace, which would present the user with a simpler, more manageable view of the tasks they need to perform.

- **Overall Interface Simplification.** All tools designed for MMC will have a similar look and feel, independent of which software vendor designed the tool.

This allows administrators to mix and match tools from any vendor to design a "toolbox" of the best tools for their needs. [Ref. 17]

d. Snap-ins

NT 5.0 Beta 1 contained a special submenu - NT 4.0 Administrative Tools - for which Snap-ins had not been created for these tools. Table 3.2 provides a summary of the available Snap-ins after Windows 2000 Beta 1 is installed. Additional Snap-ins will be included in Beta 2 and 3 and the final Windows 2000 release. A more complete list of Snap-ins is included in Appendix B. Note that Table 3.2 describes the accessible Snap-ins, which do not always correspond with the predefined MMC tools available from the Administrative Tools menu.

Microsoft has promised the following Snap-ins will be added to MMC prior to the release of Windows 2000:

- DFS
- Local user and group management
- Local security management
- Remote storage
- WINS
- Router. [Ref. 1]

The MMC Snap-ins for Windows 2000 Beta 2		
MMC Snap-in	Description	Also in Windows 2000 Professional
Computer Management	Contains the majority of functions for administering a single computer	Yes
Device Manager	Contains all information on the hardware units installed on the system	Yes
DHCP Manager	DHCP administration	No
Directory Service Migration Tool	Help tool for migration from Novell NDS to Active Directory	No
Disk Management	Disk administration	Yes
DNS Management	DNS administration	No
Event Viewer	Access to the three event logs	Yes
File Service Management	Contains vital information on file service (i.e., words, shares, sessions, and open files)	Yes
Folder	Establishes a directory in a specified place in the tree hierarchy	Yes
General Control	Capability to add an ActiveX control at a specified place in the tree hierarchy	Yes
Group Policy Editor	Administration of group policies	Yes
Index Server Management	Index Server administration	Yes
IP Security Management	Administration of the encryption possibilities on the IP level	Yes
Link to Web Address	Enables adding a binding to a URL at a specified place in the tree hierarchy	Yes
Media Services Management	Administration of new operation of the backup units that are media oriented rather than drive oriented	Yes
Microsoft Directory Service Manager	Administration of the Active Directory service	Yes
Microsoft Domain Tree Manager	Administration of the Active Directory domain tree	Yes
Microsoft Site Replication Manager	Administration of the replication setup	Yes
Monitoring Control	Adds monitor control that is used in System Monitor console, accessible from Administrative Tools menu	Yes
Schema Management	Gives access to schema for Active Directory Service	No
System Service Management	Administration of the system services	Yes

Table 3.2. MMC Snap-ins for Windows 2000 Beta 2. After Ref. [1]

Of all the tools, the Computer Management Tool is probably the most important Snap-in to administrators. It provides access to the majority of objects that administrators need to address in the daily operations of network management. This tool is used to monitor any Windows 2000-based computer from other Windows 2000 computers on the network. It does not distinguish between servers and clients, as long as the operating system is Windows 2000 and the user has the security privileges required. [Ref. 1]

The Computer Management snap-in is a remote Administrative Tools folder or remote toolbox. It not only provides access to the base Windows NT Server tools (viewing events, creating shares, managing devices, and so on), but also dynamically discovers what server services and applications there are to administrate. There are three nodes in the namespace that are provided by the Snap-in are:

- **System Tools.** Contains the tools on every Windows 2000 computer: workstation, server, domain controller, and client. These tools include Event Viewer, Service Management, Device Management and Diagnostic Snap-ins.

- **Storage.** Manages all the Snap-ins relating to disks. For Beta 1 there are no extensions of this node. Examples of future extensions are Disk Administrator and Off-line Storage Management.

- **Server Applications and Services.** Used by Snap-ins that optionally are installed on the system or are only on Windows NT Server. This node is dynamically populated depending on the computer the snap-in is focused on. For Beta 1 there are no extensions of this node. Examples of future extensions are Networking Services such as DNS, DHCP, WINS, and BackOffice applications such as SQL. [Ref. 18]

In summary, MMC will provide administrators with a "toolbox" in which they will be able to carry out specific tasks and functions. Administrators can create tools

from various Snap-ins, save those tools for future use, or sharing them with other network administrators. MMC is a core part of Microsoft's management strategy by providing a single location for monitoring and accessing all administered objects (such as users and printers) on a distributed network. Through MMC Snap-ins, administrators will gain a sophisticated interface for tracking and configuring users and resources stored in the Active Directory.

3. Microsoft Cluster Server

The Microsoft Cluster Server (MSCS) is a standard feature of Windows 2000 Advanced Server and Datacenter Server. As mentioned earlier in the Windows 2000 advanced Server section, clustering is the act of combining multiple systems (or servers) to act as a single, redundant system. The cluster configuration is managed as if it were a single server. Clustering provides high levels of availability through redundant CPUs, storage and data paths. With clustering, when one server fails, a second server can automatically pick up the failed server's workload in less than a minute, in a process known as *failover*. The monitoring services will detect the failure and shift responsibility to the designated backup server, reconnects clients and migrates shared storage and file shares. [Ref. 8].

In a typical client/server LAN environment, a single-server system provides file, print and application services to a group of desktop clients. In a cluster client/server configuration, the concept of a single server serving clients is extended to include multiple server systems. The cluster of servers is viewed by clients as a single server

system. This is accomplished via cluster software which performs the management, integration and synchronization of the servers in the cluster or cluster members. Work assigned to the cluster is partitioned across the two nodes with, for example, file services provided by one node and database services by the other. [Ref. 12]

There are currently two software models employed in clustering that affect the way nodes, or servers, share hardware: the *shared-disk* model and the *shared-nothing* model. In the shared-disk approach, software running on any of a cluster's nodes can access any disk connected to any node, as illustrated in Figure 3.7. The shared-disk model can reduce the need for peripherals and allows for easy data sharing. The shared-nothing model, as seen in Figure 3.8, assumes that each node in a cluster owns certain disks and that no direct sharing of disks between nodes occurs. Even when disks are connected to multiple nodes, as MSCS requires, only one node can own each disk. A node cannot access a disk it does not own unless the node that owns the disk fails or gives up control of the disk. The shared-nothing model improves scalability because there is no sharing to create bottlenecks, but it can increase costs because it requires more resources. [Ref. 13]

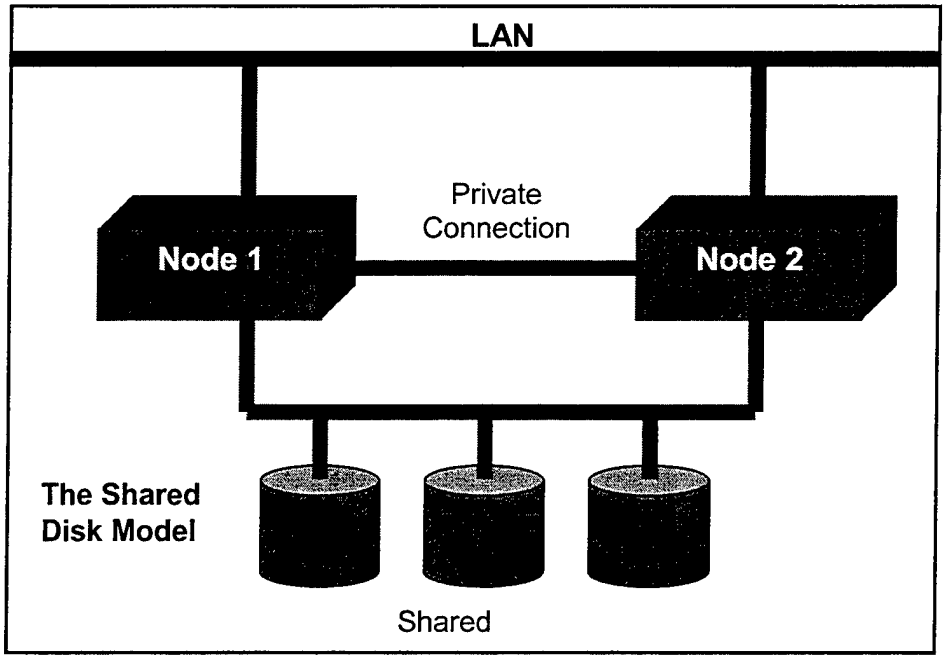


Figure 3.7. The Shared Disk Model. After Ref. [13]

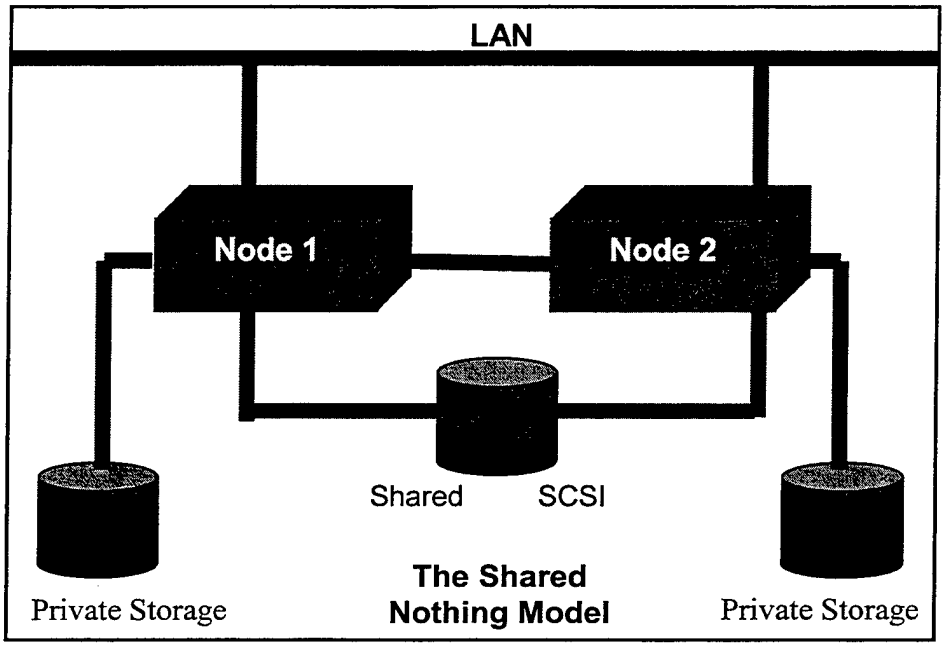


Figure 3.8. The Shared Nothing Model. After Ref. [13]

MSCS for Windows 2000 uses the Active Directory service to publish information about clusters. MSCS also takes advantage of the Microsoft Management Console (MMC) to allow administrators to visually monitor the status of all resources in the cluster. Other services such as Windows Internet Name Service (WINS), the Distributed File Services (DFS), and dynamic host configuration protocol (DHCP) are also supported by MSCS. [Ref. 14]

4. Distributed File System (DFS)

The Microsoft Distributed File System (DFS) is a new technology that provides the capability to create distributed file systems across several servers. It accomplishes this in the form of a network server component that simplifies the management and locating of data on a network. DFS makes it easy to build a single directory tree that includes multiple file servers and file shares on a network. Instead of seeing a physical network of dozens of file sharers (as in Network Neighborhood), each with a separate directory structure, users will now see logical directories that include all of the important file servers and file server shares. DFS also has the capability to place the same parts of the directory tree on several servers, adding fault tolerance to the directory tree service.

a. Distributed File System Overview

A DFS provides name transparency to different server volumes and shares. An administrator can use DFS to build a single hierarchical file system whose contents are distributed throughout an organizations LAN/WAN. In past operating systems

(including NT 4.0), a user or application was required to specify the universal naming convention (UNC) pathname to the physical server and share in order to access file information. UNCs are usually mapped to a drive letter (for example, F: might be mapped to \\Server5\Share\Path\Filename). As today's growing networks continue to use existing storage across intranets, LANs and WANS, mapping a single drive letter to individual shares scaled poorly. DFS breaks from the principle that disk partitions should always appear as a logical drive, readily accessible to users, by permitting the linking of servers and shares into a simpler, more meaningful namespace. This new DFS volume permits shares to be hierarchically connected to other Windows shares. Since DFS maps the physical storage into a logical image, the net benefit is the physical location of the share becomes transparent to users and applications. [Ref. 20]

DFS uses the existing Windows NT security model for easy administration and secure access. Participating in a DFS tree does not override Windows NT share-level security or NTFS security. Note that if a user has access to a share, he will continue to have the same level of access all the way down the DFS tree unless restricted by NTFS permissions. Each system that participates in a DFS tree controls which users have access to the resources on the system. This allows departments that have different system administrators to participate in a single tree - each administrator retains full control over the content published by their file servers. [Ref. 8]

DFS includes an administration tool, called the Distributed File System Administrator, which makes it simple to build and maintain DFS directories. This tool

provides a GUI to create replica sets, child nodes, and DFS roots. A DFS root is a local share that serves as the starting point and host to other shares. Microsoft promises to include a MMC Snap-in in future Beta and final release of Windows 2000. Table 3.3 illustrates the features and benefits of deploying DFS in a network. [Ref. 8]

Feature	Description	Benefits
Custom hierarchical view of shared network resources	By linking shares together, administrators can create a single hierarchical volume that behaves as though it was one giant hard drive. Individual users can create their own DFS volumes, which in turn can be incorporated by other DFS volumes. These are called Inter-DFS links.	Provides a simplified view of network shares that can be customized by the administrator.
Flexible volume administration	Individual shares participating in the DFS volume can be taken off-line without affecting the remaining portion of the volume namespace.	Allows administrators to manage physical network shares, independent of their logical representation to users.
Graphical administration tool	Each DFS root is administered with an easy-to-use graphical administration tool that permits browsing, configuration of volumes, alternates, and inter-DFS links, as well as administration of remote DFS roots.	Requires little training, reducing the need for trained, full-time server administrators.
Higher data availability	Multiple copies of read-only shares can be mounted under the same logical DFS name to provide alternate locations for accessing data. In the event that one of the copies becomes unavailable, an alternate will automatically be selected.	Important business data is always available, even if a server, disk drive, or file occasionally fails.
Load balancing	Multiple copies of read-only shares on separate disk drives or servers can be mounted under the same logical DFS name, thereby permitting limited load balancing between drives or servers. As users request files from the DFS volume, they are transparently referred to one of the network shares comprising the DFS volume.	Automatically distributes file access across multiple disk drives or servers to balance loads and improve response time during peak usage periods.
Name transparency	End users navigate the logical namespace without consideration to the physical locations of their data. Physical data can be relocated to any server and the logical DFS namespace can be re-configured so that the end user's perspective of the DFS namespace is unaffected (that is, it is transparent to users that their data has changed location).	Increased administrative flexibility. Administrators can move network shares between servers or disk drives without affecting users' ability to access the data.
Integration with Windows NT security model	No additional administrative or security issues. Any user that connects to a DFS volume is only permitted to access files for which they have appropriate rights on that share.	Uses the existing Windows NT Security model for easy administration and secure access.
DFS client integrated into Windows NT Workstation 4.0, available for Windows 95	The DFS Windows NT Workstation client has been incorporated into Windows NT Workstation 4.0. This integration with the SMB redirector allows the extra DFS functionality to be fully pageable, and does not affect memory needs or standard client access performance	DFS functionality requires no additional resources on client systems.
Intelligent client caching	A DFS volume can potentially connect hundreds or thousands of published shares. The client software makes no assumptions over what portion of DFS published information a user might access. As a result, the first access of a published directory caches certain information locally. The next time a client accesses that portion of the DFS namespace, the cached referral is accessed rather than obtaining a new referral.	High-performance access to complex hierarchies of network volumes.
Windows 95 and Windows 98 Client	In addition to the DFS aware Windows NT Workstation redirector that ships with Windows NT Workstation 4.0, DFS includes a Windows® 95 service to permit Windows 95 and Windows 98 users to navigate the DFS namespace. With the current release of DFS, Windows 95 clients can only access non-SMB volumes via a server based gateway (e.g., Microsoft Gateway Services for NetWare that is included with Windows NT Server).	Extends DFS benefits to Windows 95 and Windows 98 users.
Interoperates with other network file systems	Any volume that is accessible through a redirector on Windows NT Workstation can participate in the DFS namespace. This can either be through client redirectors or server-based gateway technology.	Administrators can create a single hierarchy incorporating heterogeneous network file systems.

Table 3.3. DFS Features and Benefits. After Ref. [20]

b. DFS Improvements to the Network Environment

DFS is a great improvement over drive mapping, where a network is limited to 22 drive letters (A through Z, with A, B, C, and D normally reserved for floppy drives, local hard drives, and CD-ROM drives). The improvement to the network file system is shown in Figures 3.9, 3.10, and 3.11. Figure 3.9 illustrates how an organization's data is usually spread out over many unrelated shares in a network. This leads to confusion and disorder when a user looks for files or attempts to collect data.

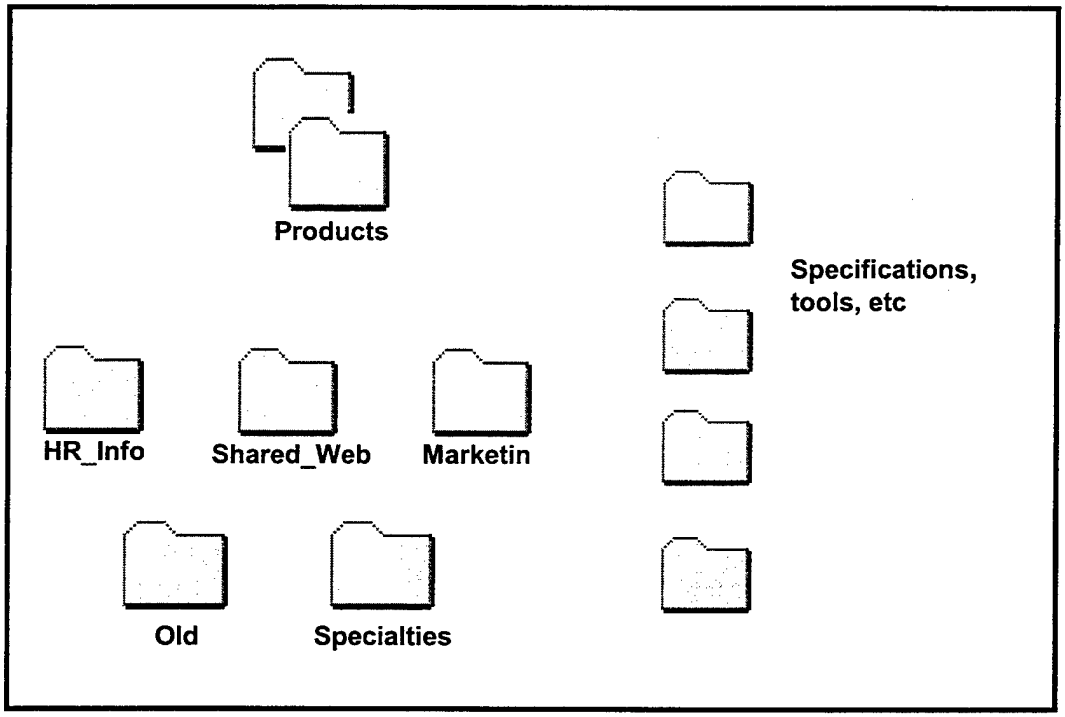


Figure 3.9. Standard share folder environment. After Ref. [1]

Figure 3.10 shows the same shares, now in a logical DFS configuration, which is a much improved organized structure. Figure 3.11 illustrates the physical implementation of the DFS share and demonstrates how several servers, each containing one or more shares, can contribute to the DFS environment. [Ref. 1]

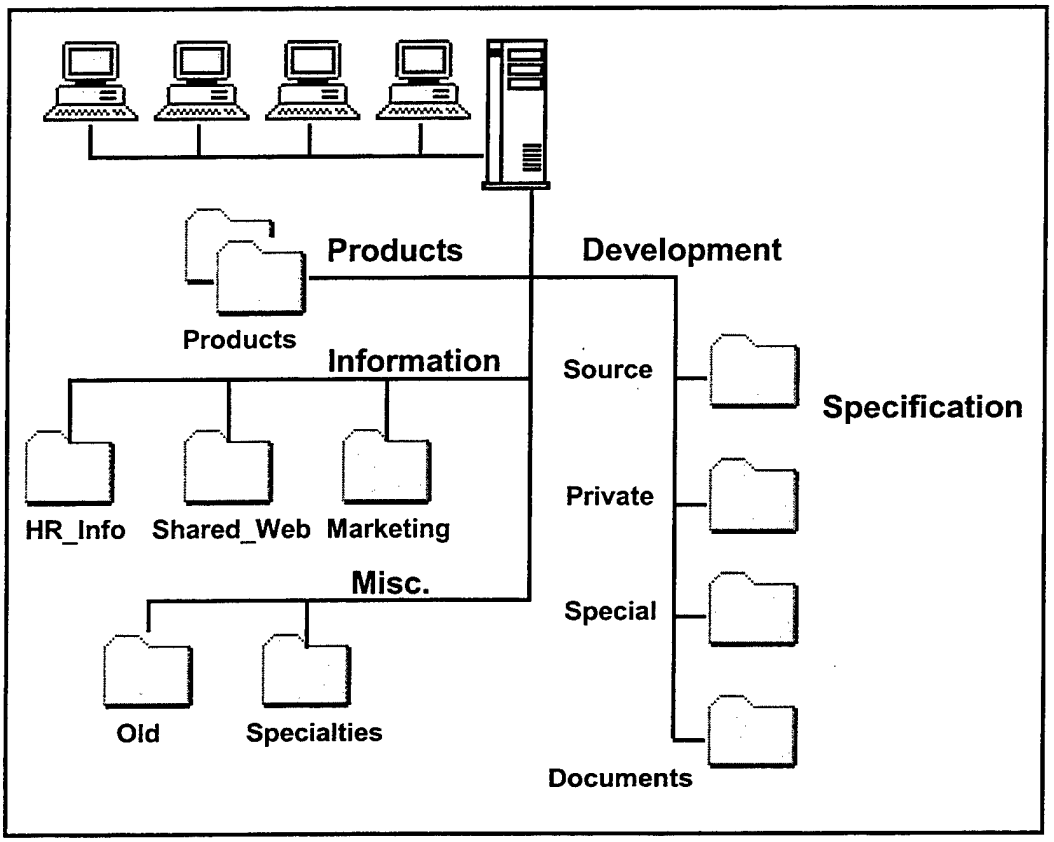


Figure 3.10. Shares collected in a logical DFS configuration. From Ref. [1]

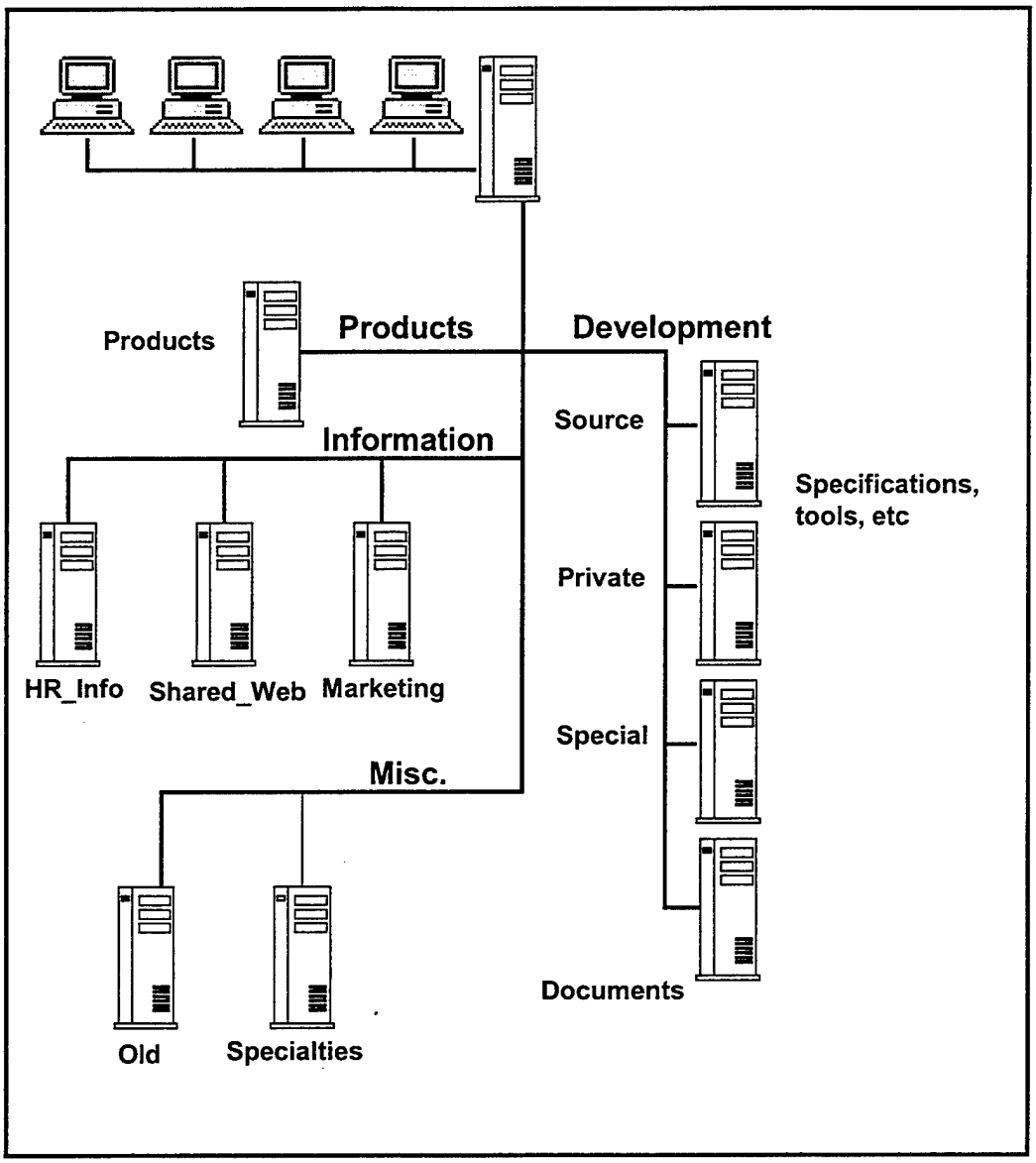


Figure 3.11. The physical network implementation of shares and partitions from Figure 3.10 spread across several servers. After Ref. [1]

(1) Fault Tolerance. DFS provides fault tolerance by allowing administrators to configure multiple Windows 2000 servers to share the same DFS root. In order to implement full fault tolerance for a DFS share, the root must be placed on a

Windows 2000 domain member [Ref. 21]. When a client connects to a DFS tree shared by multiple servers, Active Directory notifies the client software about each of the servers that share the same tree, then the client has the option of connecting to any one of the servers. If one of the servers does not respond, the client will automatically fail-over to a different server. [Ref. 1]

(2) Load Balancing. DFS provides load balancing by evenly distributing client access to DFS volumes across multiple network shares. Even if a network is part of a single DFS tree, no single server would be burdened with supporting the entire network because of this feature. Clients take advantage of the Active Directory to access site information to connect to the closest server, thus reducing the network load and the load on any given server. [Ref. 8]

(3) Replication. The Windows 2000 Server allows replication to occur between DFS roots and between child nodes. Replicas are created with the DFS Snap-in component of the MMC. Replicas must be hosted on a NTFS dynamic volume, as they will not work with FAT partitions or even Windows NT 4.0 NTFS partitions. The File Replication Service (FRS) handles the synchronization of data between shares that participate in the same replicated DFS root. The FRS automatically replicates files when they are modified and closed. [Ref. 8]

c. The DFS Architecture

The DFS root is the central component of DFS. The DFS root is the local share that constitutes the basis of the DFS file structure that receives and processes all client searches in the directory structure. For example, suppose an administrator creates a DFS root that acts exactly like a network share point. When the user chooses a subdirectory of the DFS root, the client computer recognizes the subdirectory as a placeholder for another network share. The client computer will then automatically connect to that network share, which may reside on an entirely different server.

The DFS root stores the information regarding the various shares - including mapping of logical names to physical resources - in the *Partition Knowledge Table (PKT)*. The PKT is cached locally onto client computers to achieve a higher lookup speed and to lower the load on the DFS root. It is important to note that only one DFS root can be placed on each server.

The attachment to each share is known as a *junction point*, a logical connection between two separate network points. Junction points are used in the NT File System (NTFS) to link together volumes across several servers, similar to DFS, but NTFS junction points only contain a small part of DFS functionality. Figure 3.12 shows the overall DFS implementation, including how junction points function to bridge two servers, and the root-branch structure for each server. [Ref. 1]

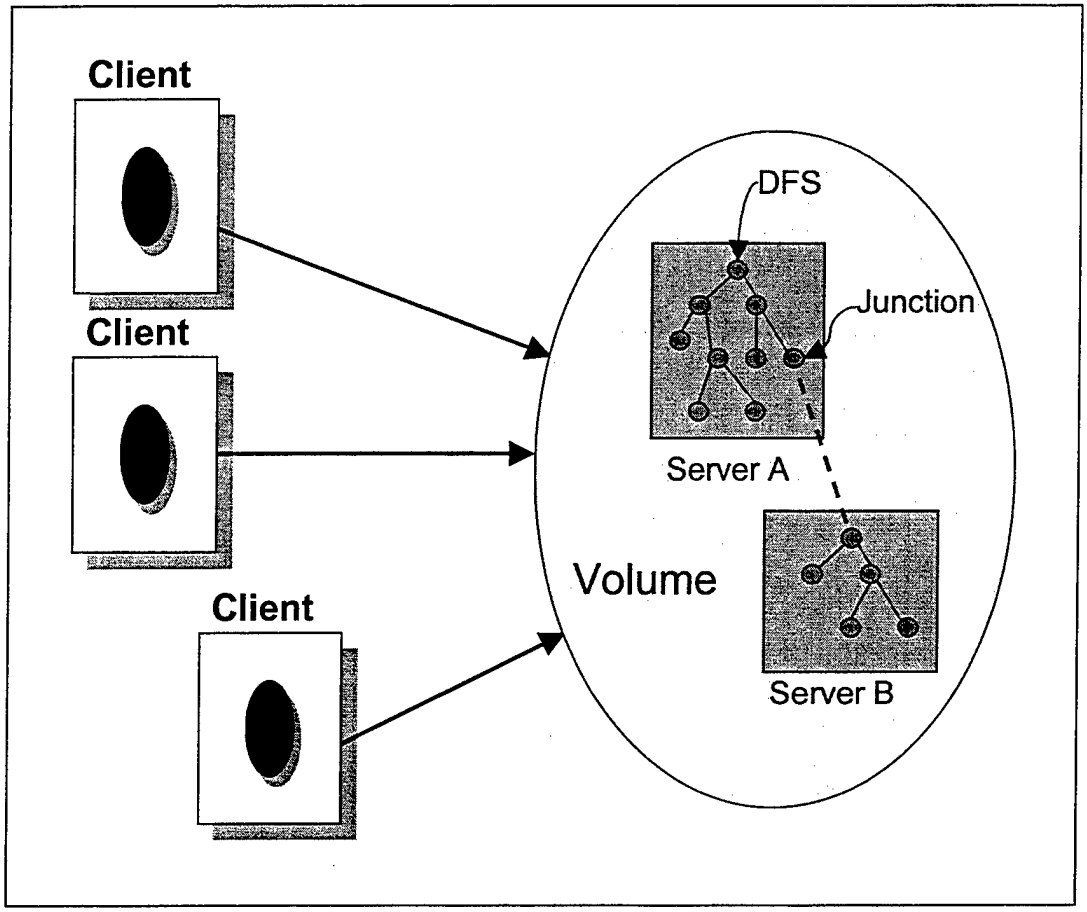


Figure 3.12. An overall picture of DFS implementation. The junction-point is the logical connection between two separate network points. After Ref. [1]

d. DFS Solutions

DFS is useful in many situations, but its strength is most noticeable in two frequently encountered situations: when you run out of disk space or the network environment is decentralized.

In the first situation, when a network runs out of disks in the file server or on the disk controller, it may not be possible to introduce a new server with a new share. DFS allows the file server to remain as it exists and the addition of a new server that takes

over part of the existing file system. This solution is very easy to implement, with the addition of enhanced performance.

The second situation DFS can be highly useful is in a very decentralized business in which individual departments have their own file servers and do not wish to change the setup. Instead of implementing a multitude of drive mappings to the various shares, DFS would allow the collection of all shares into one file structure, in which every subdirectory is assigned a descriptive name (for example, to match the departmental structure) that corresponds with each of the decentralized servers.

5. NT File System (NTFS)

NTFS (remember, NT stands for New Technology) was created specifically for Windows NT; in fact, only Windows NT and Windows 2000 operating systems support NTFS. NTFS offers many advantages over FAT, including fault tolerance, security, support for large file and partition sizes, and file compression. Windows 2000 features an upgrade to the existing NTFS volumes found in Windows NT 3.x-4.0 environments. When Windows 2000 is installed, existing NTFS volumes are upgraded to NTFS version 5.0. This newer version includes capabilities such as disk quotas for users, encrypted files, journaling and other features that Windows 2000 components and services rely on to function correctly.

Upgrading the NTFS file system is mandatory; all local NTFS volumes, including removable media, are upgraded to NTFS 5.0. If the administrator wants to configure the system to run Windows NT 4.0 and Windows 2000, the system must first be upgraded to

Windows NT 4.0 with Service Pack 4 installed. New features of the NTFS 5.0 file system are discussed in the following sections.

a. Disk Quotas

Disk quotas enable administrators to limit the amount of disk space users can consume on a per-volume basis. This level of control can prevent common storage problems, such as running out of disk space, before they occur. It will also prevent any single user from monopolizing a disk, share folder, or volume. Windows 2000 calculates quota limits and thresholds by file ownership, and is tracked on a *per-user per-volume* basis. Disk quotas can only be assigned to volumes, not disks, nor can they be set to individual files or folders. Also, disk quotas are based on uncompressed file sizes, so compressing data will not increase the amount of free space available to users.

b. Encryption

NTFS 5.0 can automatically encrypt and decrypt file data as it is read and written to the disk. The encryption does not occur on NTFS itself, but is done through a component called the Encrypting File System (EFS). EFS enables security-conscious organizations to use file and directory level-encryption for added privacy, though the users will not be see any visible difference between encrypted and decrypted files. EFS is based on public-key encryption, which is discussed in Chapter V (Windows 2000 Security Features).

c. Dynamic Disk Storage

Dynamic disk storage enables administrators to assign or remove disk space from various volumes and logical drives, or add new disks without rebooting the operating system. Dynamic disks are organized in volumes and have no partitions or logical drives.

Two other volumes introduced in Windows 2000 enable administrators to separate the fundamental Windows 2000 components from other files on the disk level. They are the System Volume, which contains the hardware-specific files necessary to input Windows 2000, and the Boot Volume, which contains all the Windows 2000 system files placed in the \System32 subdirectory.

d. Additional Features

NTFS offers several other features which are mentioned below:

- **Sparse Files** - allow programs to create very large files but to consume disk space only as needed.
- **Reparse Points** - Reparse Points are symbolic links that can point at files or directories on the same or other disks.
- **Auditing** - Enables administrators to select events that trigger Windows 2000 to record information to an audit trail.
- **Journaling** - Provides a persistent log of all changes made to files on a volume. This feature is one reason why Windows 2000 domain controllers must use an NTFS 5.0 partition as the system volume.
- **Disk Defragmentation** - Prior to Windows 2000 and NTFS 5.0, no native capability to defragment NTFS drives existed (although third-party software is available). Administers can initiate defragmentation manually and only on a local system. [Ref. 21]

These new features are only available with Windows 2000 and NTFS version 5.0 installed. By implementing NTFS 5.0, the file system will maintain maximum integration with the rest of the operating system and be able to take advantage of all the built-in advantages of both.

C. CHAPTER SUMMARY

While Windows 2000 offers countless new features and takes advantage of the newest technologies available, these features discussed are arguably the most important concepts to understand. If the network administrator understands the basic philosophy behind each server operating system and understands the major new features, and what impact they will have on a network, then they can plan for the future with Windows 2000 in mind.

The addition of Active Directory to a network environment is a significant improvement over older service to manage network resources. This feature, plus the addition of Microsoft Management Console and the Distributed File System provide Windows 2000 with powerful administrative and user-level tools that will, in the long run, make careful planning and preparation for Windows 2000 by any organization very productive.

IV. PREPARING FOR WINDOWS 2000

Planning a Windows 2000 Server infrastructure will require administrators to carefully plan the changes needed to make a successful transition to Windows 2000. This study has focused on the new technologies and features that make the Windows 2000 Server family an innovation in network operating systems.

This chapter introduces strategies to aid administrators in preparing their network for Windows 2000, focusing on upgrading from Windows NT 3.X/4.0. Critical areas to be discussed are restructuring existing Windows NT domains, designing a network for the deployment of Windows 2000, and the actual deployment of the operating system itself.

A. RESTRUCTURING EXISTING DOMAINS

Possibly the most challenging element of deploying Windows 2000 is the requirement to restructure existing domains in the network. The process could involve combining two domains into one, combining multiple domains, and moving applications from one domain to another.

Administrators need to understand the strategy involved in restructuring *downlevel* domains. A downlevel domain is a domain based on Microsoft technology released prior to Windows 2000. Windows NT 3.x - 4.0 domains are the most popular downlevel domains existing in today's networks. This section describes the importance

of understanding the downlevel domain models and how restructuring them will simplify the migration process.

1. Downlevel Domain Models

In Windows NT networks, multiple domains are created most often for two reasons: to delegate administrative tasks, and in much larger networks, to work around the Security Accounts Manager (SAM) database limitation of 40 MB. An overview of the common downlevel domain models follows. Note that the single domain model is not included - if an organization has only one domain, then no restructuring is needed in preparation for Windows 2000.

a. The Single Master Domain Model

The single master domain model is probably the most widely implemented NT domain. It consists of two types of domains:

- Master Domain - domain where all user accounts are centralized.
- Resource Domains - Includes decentralized resources allowing administrators in the resource domains to administer their own resources.

Resources are objects the clients require access to for specific jobs. These resources are commonly found on servers, including file shares, printers, and applications such as databases, web servers, and e-mail servers. All resources reside in the resource domains while all user accounts reside in the master domain. Resource domains trust the master domain in a one-way trust relationship. A trust is an administrative link that

combines two or more domains. A trust allows a user in one domain to access a resource in another domain without having a user account in both domains. A one-way trust only provides access in one direction. Figure 4.1 illustrates a single master domain with three resource domains. Each of the resource domains trusts the master domain. All the users in the master domain have access to each resource domain. A point to remember is that there can be many resource domains but only one master domain is allowed.

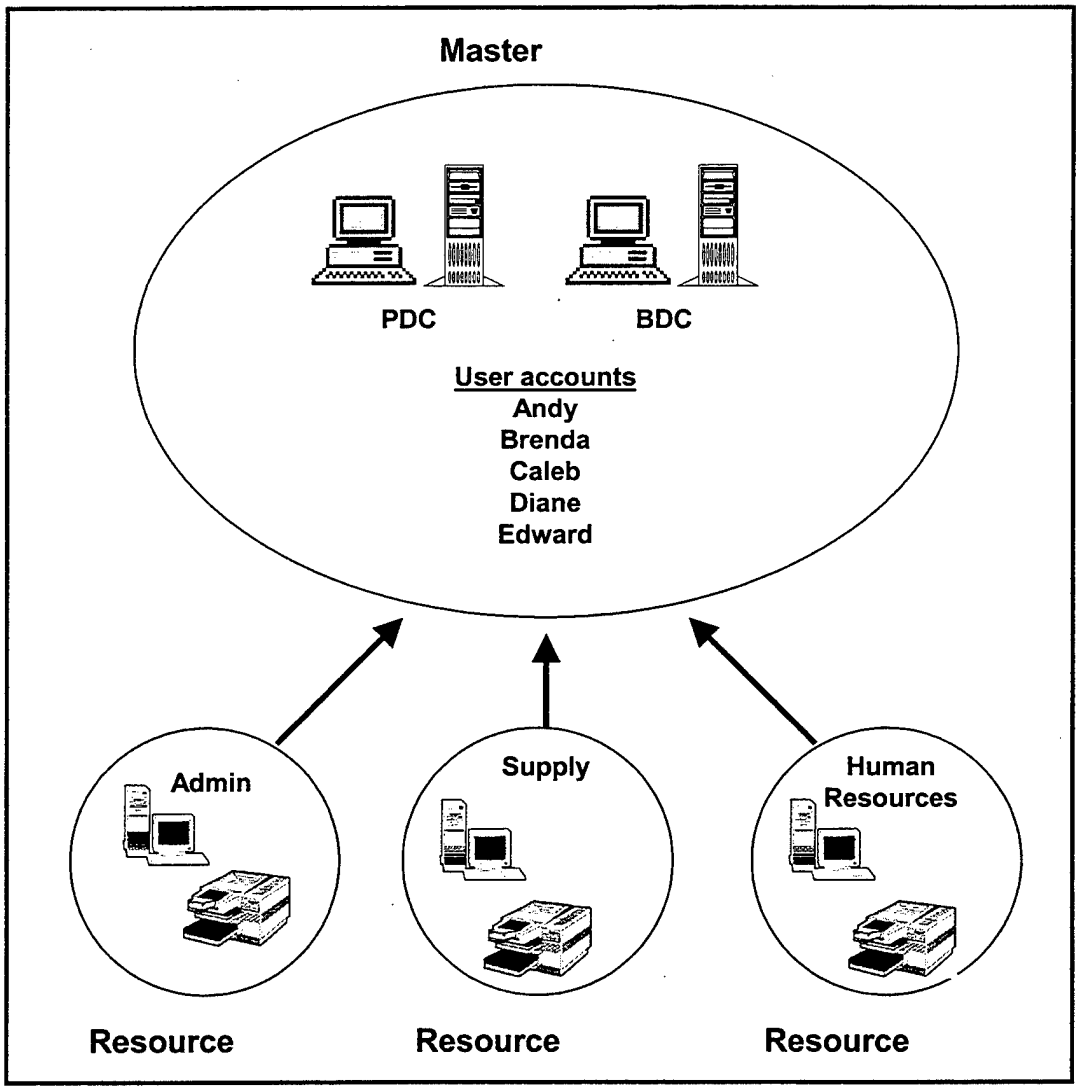


Figure 4.1. The Single Master Domain Model.

b. The Multiple Master Domain

The multiple master domain model forms an administrative hierarchy. The resource domains in this model serve the same purpose as those in the single master domain model. The difference is the number of master domains allowed. The use of multiple master domains is driven by the limitations of the SAM database, which should never be larger than 40 MB. The SAM database is made up of the following objects:

- User accounts - 1 KB each
- Computer accounts - 0.5 KB each
- Global group accounts - 0.5 KB each
- Local group accounts - 0.5 KB each. [Ref. 22]

A master domain with 20,000 user accounts, 20,000 computer accounts, 500 global group accounts, and 500 local group accounts would nearly surpass the 40 MB limit. If an organization has more than 20,000 users it is a good idea to create multiple master domains. Multiple master domains allow an NT network to overcome this limit and still provide networking services. Multiple master domains are commonly used in large organizations with many users, or when companies merge, providing the simplest way to combine domains. Figure 4.2 illustrates the multiple master domain model.

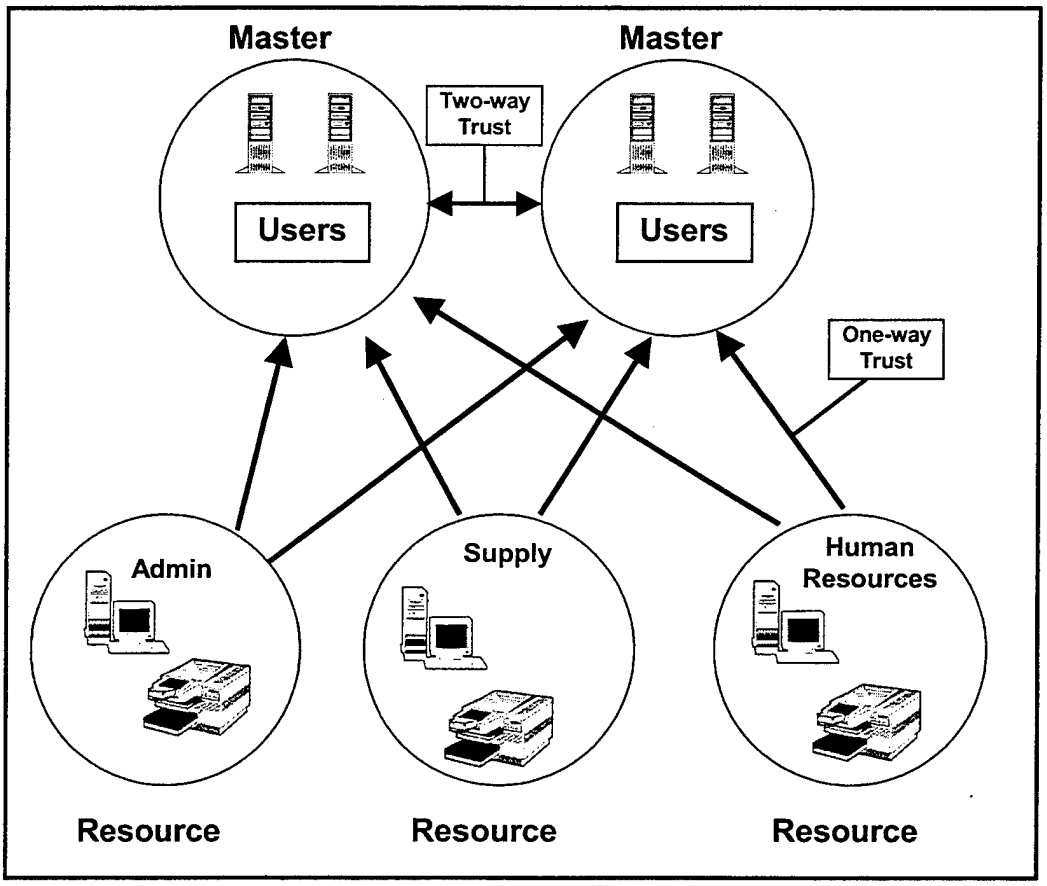


Figure 4.2. The Multiple Master Domain Model.

Two-way trusts exist between all the master domains, and one-way trusts exist between the resource domains and each master domains. A two-way trust is set up between two domains when bi-directional access is required. Two-way trusts are required between each of the master domains in the multiple master domain model.

c. The Complete Trust Domain Model

The complete trust domain is made of several independent domains, with a two-way trust between every domain. It allows decentralized account management and assumes that accounts and resources are located in each domain. There is no

administrative hierarchy between the domains such as those formed in single and multiple master domains. User accounts and resources exists in each independent domain. This type of domain exists in organizations that require completely decentralized administration but also require resource sharing across multiple domains. A company without a central Management Information Services (MIS) department could use the complete trust domain model to ensure resource sharing. The greatest drawback to this model is the complexity required to provide the two-way trusts to all domains. Figure 4.3 illustrates the complete trust domain model.

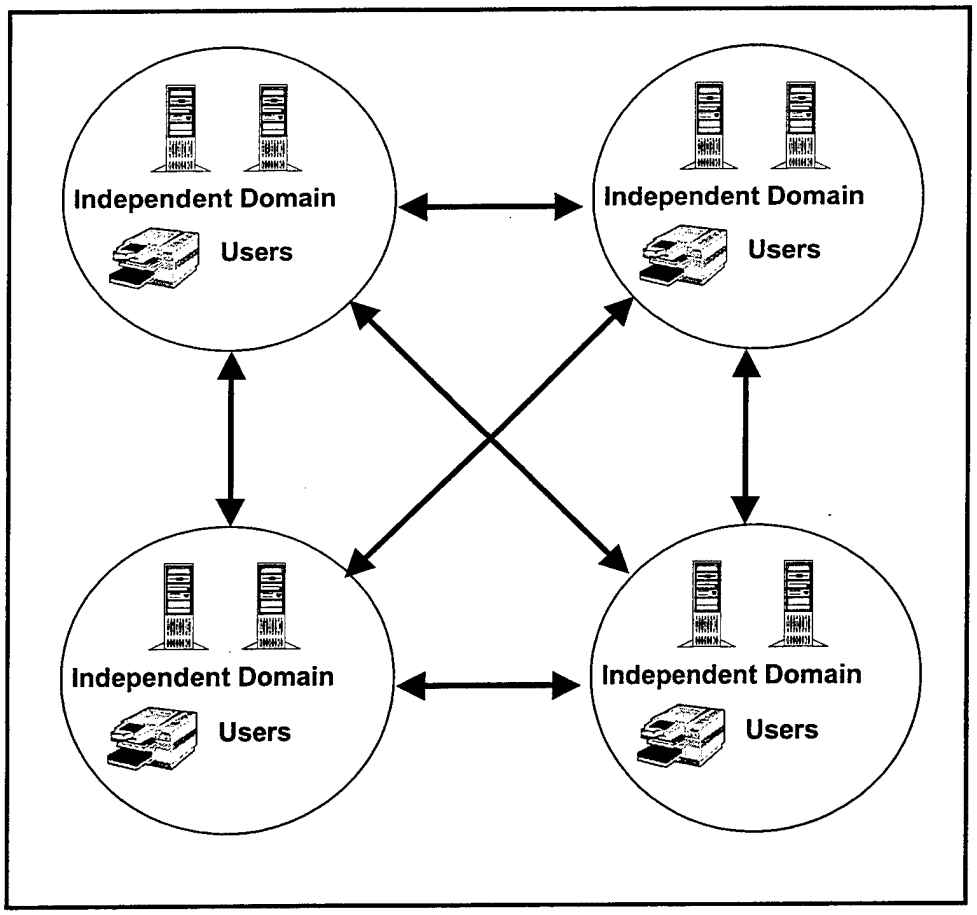


Figure 4.3. The Complete Trust Model.

d. The Ideal Domain Model

Simply put, an Ideal domain is one that mirrors the Active Directory design for the network. This model will upgrade to the domain defined in the Active Directory design with little preparation. For example, if the Active Directory design calls for two domains, and the physical implementation is three domains, the domains and Active directory do not match. An administrator would have to consider either eliminating the extra domain or updating the Active Directory, which would be a significant chore. Active Directory and how it can be used in the migration process is discussed in the next section, Designing Windows 2000 Networks.

2. Restructuring Options

There are two basic options to restructuring an organization's domains:

- Restructuring domains before an upgrade
- Restructuring domains after the upgrade

To determine when to combine domains, you need to consider the number of domains to be eliminated and the available resources. For example, if your plan is to combine a large number of domains to mirror the Active Directory, combining some domains before upgrade may be in order. However, this should be done only if the number of available resources is sufficient to allow for the loss of some resources. The following guidelines are offered for determining the best method:

Restructuring Option	When to Start
Combining more than thirty percent of your existing domains	Before your Windows 2000 upgrade
Combining fewer than thirty percent of your existing domains. [Ref. 21]	After your Windows 2000 upgrade

Note that Windows NT 3.x - 4.0 has no built-in tools to move objects between domains. Administrators have to use utilities from the NT Resource Kit or third- party tools. While no formula works for all organizations, it is commonly more difficult to combine domains before upgrading to Windows 20000 than afterward.

a. Restructuring Domains before Upgrading

Even if domains are not combined before an upgrade, the transition to Windows 2000 could still be an extremely complex task. Some issues to aid in your decision of when to upgrade are:

- Never combine domains if the combined SAM database will be greater than 40 MB.
- When domains are combined, the SAM database will increase in size, and SAM replication will increase accordingly. Ensure that the network can handle the additional traffic.
- Some domains may have been created along administrative guidelines vice physical limitations. If these domains are eliminated, the current administrative model will be changed. [Ref. 21]

Combining domains can be an extremely complex task. The process involves making significant changes to your existing environment, such as modifying user and group accounts, file permissions, user rights and policies, and more. Each step

in the combining process is important not only in itself but also in the order in which they occur. For a successful restructuring before upgrading to Windows 2000, the following ordered steps may prove a useful guide to combining domains:

- **Step 1: Migrate user accounts.** You must migrate users from your source domain to your target domain. This requires the administrator to create a new user account in the target domain for every user that exists in the source domain. The command line utility ADDUSERS.EXE will accomplish enable this process to be completed reliably.

- **Step 2: Migrating Global Groups.** Migrate global groups from the source domain to the target domain. This requires the administrator to create a new global account in the target domain for each global group in the source domain, then to associate users with the global groups. ADDUSERS.EXE can be used to copy groups also.

- **Step 3: Updating Local Group Memberships.** Add users and global groups from your target domain as members of local groups in your source domain. These local groups can exist on domain controllers, member servers, and NT workstations in the source domain. ADDUSERS.EXE can be used to update local groups.

- **Step 4: Updating Permissions.** Update permissions for resources in the source domain to reflect accounts in the target domain. These include permissions for files, shares, and directories on computers in the source domain that will move to the target domain. This step can be challenging because of the broad scope of the task. The SIDWalker Tools are included in the Windows 2000 Resource Kit to support this task.

- **Step 5: Updating User Rights.** Update the user rights in the source domain to reflect the accounts in the target domain. This step consists of changing user rights on every domain controller, member server, and NT workstation that will migrate from the source domain to the target domain. The command line utility NTRIGHTS.EXE can be used to update user rights.

- **Step 6: Migrating Computer Accounts.** Create new computer accounts in the target domain in order for computers in the source domain to join the target domain. To migrate computer accounts, use the utility NETDOM.EXE.

- **Step 7: Moving Domain Controllers.** Domain controllers can now be moved from the source domain to the target domain. If a domain controller,

such as a PDC or BDC, has the sole purpose of authentication logons, it is not required to be moved to the target domain. The PDC or BDC should be left running in the source domain until all the member servers and workstations have migrated to the target domain.

- **Step 8: Moving Member Servers.** First, verify that steps 1-6 have been completed. If any steps have been skipped, user rights and permissions will not reflect the accounts in the target domain.

- **Step 9: Moving Workstations.** The final step is to move workstations from the source domain to the target domain. Verify that steps 1-6 have been completed or the permissions and user rights will not reflect the new accounts in the target domain. Workstations can be manually moved by accessing the Network Identification tab (under Network Settings control panel), or can be automated by using the NETDOM.EXE and SHUTDOWN.EXE utilities. [Ref. 21]

b. Combining Domains After Upgrading

If combining domains after upgrading to Windows 2000 is most suited for a network, then the first step is to move applications and services from domain controllers to member servers in any domains that will be eliminated. This process is as follows:

- **Step 1: Designing the Migration Plan.** Design an application and service migration plan. This may involve building a lab to capture the scope of the migration effort. This will help determine what affects occur when applications or services are moved to member servers.

- **Step 2: Forming Back Out Procedures.** Once the migration plan is designed, it is strongly recommended to design a back out plan. This is simply a plan to reverse the migration process in the event of serious problems during the actual migration. This will require the domain controller to be restored back to its original state prior to migration. An acceptance plan that establishes whether a migration is successful should also be implemented. The acceptance plan can be a series of practical system checks or simple end-user usability tests. Finally, benchmarks should be set for determining a failed migration, thus causing the back out plan to be implemented.

- **Step 3: Testing the Migration Plan.** Test the migration and back out plans in the experimental lab. Refine the steps so they are clear and concise, then follow them exactly.

- **Step 4: Executing the Migration Plan.** Be thoroughly prepared for this step by ensuring all details have been included in the migration plan. It is recommended to make backups of the computers before any changes to the computers are made. Follow the migration plan verbatim with no deviation. The back out plan and full backups will aid in recovery if the migration fails.

- **Step 5: Performing Acceptance Testing.** After a successful migration (yahoo!) perform the acceptance test plan. This will verify what should be obvious- a successful migration. Verify permissions and user rights to applications and perform end-user testing.

- **Step 6: Removing the Source Domain.** After moving the applications and services from domain controllers to member servers in the source domain, it can now be combined with the target domain. Note that if these applications and services can be moved to member servers before updating to Windows 2000, eliminating a domain will be much easier. [Ref. 21]

B. DESIGNING WINDOWS 2000 NETWORKS

Designing a network for Windows 2000 involves careful planning precise and implementation of services. This section will provide an overview of some of the important requirements for a successful deployment of Windows 2000. Topics discussed include designing the Active Directory, Dynamic Domain Name Service (DDNS), IP addressing, and hardware concerns.

1. Designing the Active Directory

Windows NT networks are fundamentally different from those designed for Windows 2000, especially when the Active Directory environment is introduced. In

order to migrate a network to Windows 2000, several areas of Active Directory design concepts must be considered. The following sections offer an overview of the planning process needed to successfully design a network based on Active Directory.

a. Planning a Domain Structure

In downlevel domains, the domain structure is reflected in the relationship between the master domains and the resource domains. Networks were based on one of the four domain models: single domain, single master domain, multiple master domain, and the complete trust domain. As stated earlier, the SAM database could impose limitations on what type of domain model an organization used. Windows 2000 does not have this limitation. The Windows 2000 domain structure should be based on the operational or physical structure of the organization, provided that this design parameter is also used in the organization model of the organization. [Ref. 1]

The advantages of placing all objects in one domain are straightforward. With all objects grouped in one domain, any domain controller can handle all queries. The requirement to administer several relationships between domains disappears. Also, the possibility to divide a domain into divisions, operational areas, departments, workgroups, or other functional areas, remains an option.

The disadvantage is that replication of the Active directory database can be cumbersome. The entire Active Directory database must be replicated onto all domain controllers within the same domain, requiring large amounts of bandwidth in large organizations. Active Directory overcomes this disadvantage somewhat by replicating

only the properties that have changed since the last replication. When Active Directory replication occurs within sites can also be controlled. [Ref. 1]

b. Organizing Domains in Trees or Forests

After establishing the number of domains appropriate for the organization, a decision must be made whether to arrange the domains into a Tree or a Forest. The Tree or Forest forming the domain namespace represents the network's logical structure. Some companies or organizations need a single tree to support their enterprise, while others may require a Forest of Trees. Trees and Forests both form a structure in which every domain shares the same configuration, global catalog, and schema. When a new domain is joined to this hierarchy, it establishes a two-way trust relationship with its parent, therefore sharing all resources.

There are more differences than similarities between Trees and Forests. Table 4.1 illustrates the differences between the two structures.

Trees	Forests
Form a single contiguous namespace Useful for companies that operate as a single entity	Made of several namespaces Useful for companies that operate as several entities, such as partnerships, holding companies, conglomerates, and joint ventures
Simpler for users and administrators to navigate and understand	More difficult for users and administrators to navigate and understand
LDAP searches in a Tree can always be resolved by LDAP referrals	LDAP searches in a Forest will not always be resolved. Forest searches are limited to replicated attributes in the global catalog and objects in the Tree from which a search is initiated

Table 4.1. Distinctions Between Trees and Forests That Affect the Organization of Domains. After Ref. [21]

c. Planning an Organizational Unit Structure

After determining the design domain strategy, the next step is to arrange its OUs. When the domain is split into a hierarchy, you no longer have to look at resources in a flat list. The OUs allow you to organize objects into logical structures that fit into the way a company is organized. Using OUs could also reduce the number of domains necessary by establishing an Active Directory that is identical with the corporate structure of the organization.

d. Planning a Site Structure

While Trees and Forests define the logical structure, sites define the physical structure of a domain. Sites are placed in a separate part of Active Directory because they relate only to hardware components, such as computer objects and attachment objects. An organization's site objects are used to define areas of good network connectivity, and are associated with one or more TCP/IP subnets. Each subnet defined in Active directory should share a high bandwidth link (512Kbps or greater).

Site objects can be used for the following reasons:

- **Throttle replication traffic.** Intra-site replication is used within a site, in which a ring topology is defined with a minimum of two replication paths among domain controllers for added redundancy. Inter-site replication is used to synchronize domain controller in separate sites and is always compressed.
- **Isolate logon traffic**. During the logon process, a workstation interrogates the site objects in Active Directory to find a domain controller in the local site. Defining different sites in the same physical location allows an administrator to more closely control the logon process.
- **Identify Resources by Proximity.** Sites are used to find other resources within close proximity, such as a nearby global catalog server. [Ref. 21]

2. Planning a Dynamic DNS Structure

Microsoft offers a new solution to name resolution in Windows 2000, called Dynamic Domain Name System (DDNS). This is an entirely new version of DNS, an open Internet standard that translates textual Internet network addresses into IP addresses. DNS is currently the preferred name resolution standard of the Internet and Intranets.

Windows NT networks have relied on the Windows Internet Name Service (WINS) to resolve NetBIOS names to an IP address. The reason is simple: WINS provided support for clients that used dynamically assigned IP addresses. Windows NT 3.x-4.0 systems require NetBIOS to gain access to the services for sharing files and printers. In order for TCP/IP to be used as a basic protocol in a Windows NT network, NetBIOS had be used over TCP/IP, which required a WINS server to be installed. Therefore, Windows NT networks have two name resolution conventions: WINS, for internal name resolution, and DNS, for Internet name resolution. With Microsoft's introduction of DDNS, WINS will no longer be required, though it remains a part of the Windows 2000 server operating systems to ensure downlevel compatibility.

a. Planning the DDNS Namespace

When designing a network in preparation for Windows 2000, the design goals for DDNS and Active Directory should be identical. To help in defining the DDNS namespace, some common DNS design standards are as follows:

- The top-most domain should remain static. This domain will usually be the name of the organization, such as **microsoft.com**.
- International organizations often divide the DNS namespace into subdomains to delegate administrative task.
- Subdomains are created most often to represent geopolitical boundaries, distinct administrative lines, or business units.
- Subdomains can be created to mirror the IT support structure. [Ref. 21]

DDNS offers greater flexibility and alternatives than DNS, so basing the DDNS design on DNS standards may be difficult. The most likely solution to designing a DDNS namespace is along any existing organizational or natural divisions. One factor to consider is the division of subdomains. If the organization is currently ordered into 12 divisions, forcing them into six subdomains to simplify administration may just confuse the users. Another factor to consider is whether the subdomain plan matches the Active Directory domains. If these do not match, a compromise must be made. Normally Active Directory domains criteria outweigh those for forming DDNS domains. [Ref. 21]

An important decision to make in the planning stage is whether to have the same or different internal and external namespace. Both have pros and cons, but it is more common for organizations with an Internet interface to have separate internal and external domain names. The organization in Figure 4.4 uses **navy-recruiter.mil** outside the firewall and **rhq.navy.mil** inside the firewall. By using different internal and external namespaces, privacy is provided for internal resources while simplifying the name resolution process. Also, there is no need to mirror external servers (such as ftp or web servers) inside the firewall or to configure proxies to differentiate between external servers and mirrored servers. [Ref. 21]

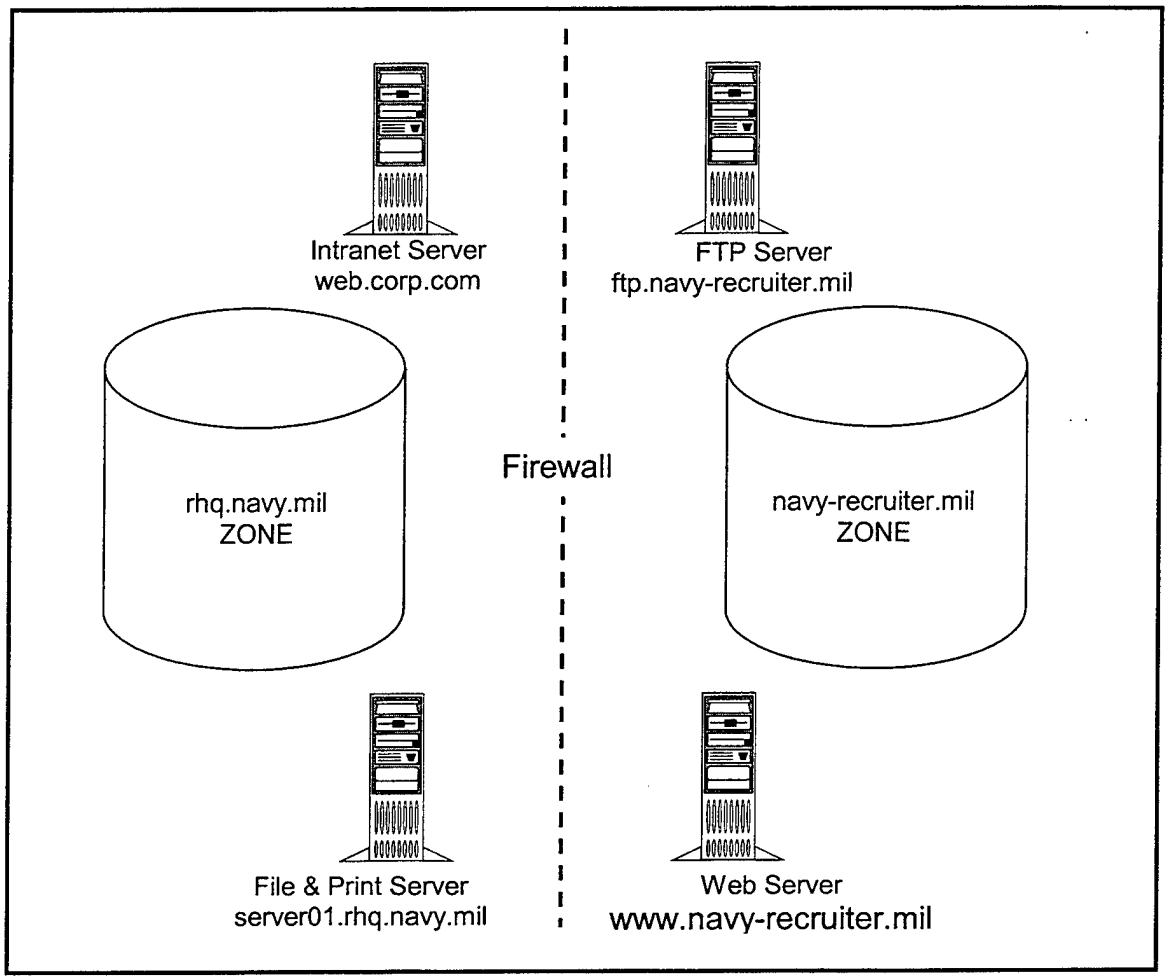


Figure 4.4. Different internal and external namespaces used in a network. After Ref. [21]

The first DDNS zone is set up outside the firewall and provides name resolution services for the **rhq.navy.mil** domain. The second DDNS zone is placed inside the firewall and resolves all names in the **navy-recruiter.mil** domain. Users are able to differentiate between internal and external resources based on their Fully Qualified Domain Name (FQDN). Both domain names need to be registered on the Internet separately to prevent either name from being used by someone at a later date.

b. Creating DDNS Naming Standards

Choosing a name for DDNS domains and subdomains is not an easy task. Selecting a name for sub-level domains is a critical step in DDNS implementation, as it will form the root of the Active Directory Tree or Forest and is the top-most domain name in DDNS. Changing this name later will be difficult and could lead to confusion among users.

Second-level domain names are commonly chosen as a representative of the organization's identity. Such as **microsoft.com** or **nps.navy.mil**. This name should be registered on the Internet through the InterNIC. Most importantly, the second-level domain should remain static.

c. WINS and DDNS Integration

Integrating WINS and DNS in downlevel domains has become a standard practice. Though WINS is not required in Windows 2000, integrating WINS and DDNS can help in certain situations:

- It can prove helpful if there is a requirement to support downlevel clients during the Windows 2000 transition.
- A Windows DHCP server can update DDNS with the IP addresses of downlevel clients. In this configuration, a downlevel client can be found by querying both DDNS and WINS.
- If Windows 2000 is not used for the download client's DHCP server, you should configure DDNS for WINS lookup. This will allow you to query DDNS to resolve downlevel names to IP addresses. [Ref. 21]

The WINS lookup feature dynamically manages the mapping between friendly names and IP addresses of network resources. If the name of a downlevel client cannot be resolved using DNS, the name request is forwarded to WINS for resolution. Enabling WINS lookup allows DDNS to use WINS to look up names that cannot be found in the DDNS server's database. WINS lookup can be used in Windows 2000 to help non-Microsoft operating systems to find WINS clients. For example, a Unix client can query DDNS to resolve a downlevel server's dynamic IP address. Furthermore, WINS lookup is required for a Windows 2000 client to map a downlevel share, printer, or other downlevel resource. [Ref. 21]

d. Planning DHCP Services

One of the reasons that DDNS supports dynamic update is for an enhanced integration with DHCP. Windows 2000 DHCP servers support several new functions, such as storing static IP entries in Active Directory and running on a Microsoft Cluster Service (MSCS) server. There are many advantages to using DHCP over static IP addressing; the most obvious being that DHCP prevents IP addresses from being duplicated. DHCP is arguably a requirement in Windows 2000 networks, as it will provide solutions more accurate and less troublesome than managing a static IP pool.

The following actions should be taken to ensure a proper DHCP deployment in a Windows 2000 environment:

- **Determine the number of DHCP servers required.** One DHCP server can support many clients, but it is common to provide fault tolerance for DHCP servers by implementing backup servers for one or more scopes (pools of IP

addresses). Windows 2000 DHCP servers are cluster-aware, allowing them to be instantiated on one cluster member if the other becomes unavailable.

- **Define and configure scopes.** Scopes are normally created for each IP subnet. Scopes are usually designed around the needs of the endusers, allowing a pool of addresses to be excluded from the scope or giving certain users a longer lease duration.

- **Reservations.** Reservations ensure that a DHCP server does not attempt to lease an IP address that is statically allocated. Static hosts are still common for WINS servers, DDNS servers, print servers, and Unix hosts. [Ref. 21]

DDNS will likely prove extremely successful in the coming years, especially as Windows 2000 becomes stronger in the network market. No real alternative to DDNS is in development. Though DDNS is in its infancy, the Internet Engineering Task Force (IETF) recognizes it as an official Internet standard and its implementation in Windows 2000 means that DDNS will only gain momentum.

3. Hardware Needs

When preparing a network for Windows 2000, the two greatest hardware concerns are if the existing hardware is compatible, and is the hardware powerful enough to perform at acceptable levels under Windows 2000. This section discusses steps to take to analyze a network prior to upgrading, and also offers solutions for some common problems encountered when preparing a network for Windows 2000.

a. Analyzing Current Systems

While network servers may perform satisfactorily for Windows NT, they will not necessarily perform well for Windows 2000. For example, Windows NT 4.0 requires a 486 CPU with 16 MB of RAM as the minimum hardware, though 32 MB is recommended. Windows 2000 requires a Pentium 166 MHz CPU and 64 MB of RAM, with 128 MB required for acceptable performance. The increase in RAM requirements is due to the many features and services offered by Windows 2000 over that of Windows NT. Active Directory alone places greater demands on hardware than one Windows NT domain controller.

Windows 2000 depends on four system components to ensure satisfactory performance. Any one of these critical areas - CPU, memory, mass storage, and network connectivity- can degrade performance and cause bottlenecks.

- **CPU(s).** If the network is performing well with the current CPU, chances are it will continue to do so with Windows 2000. However, if the server will be offering new functionality, an upgrade may be in order.

- **Memory.** The majority of server performance problems can be traced to lack of memory. Any system with less than 128 MB is not likely to perform well under Windows 2000. Remember that the new features in Windows 2000 require approximately 32 MB more RAM than Windows NT systems.

- **Mass Storage.** Windows 2000 will have roughly the same disk performance as Windows NT. Since Windows 2000 systems require more RAM, they will also require a larger paging file. Windows 2000 also requires more space for the operating system than Windows NT. Windows 2000 requires 500 MB of free space compared to 125 MB for Windows NT.

- **Network Connectivity.** Many Windows 2000 servers will require more bandwidth due to Active Directory and other network services. If the current

network has plenty of available bandwidth for both servers and clients, there shouldn't be any noticeable loss in performance. [Ref. 21]

b. Upgrading or Replacing Components

A question all network administrators must answer is to upgrade components or replace the entire computer. Upgrading can be less expensive, and if a system is near perfect, except for one or two areas, upgrading is probably a better choice. However, when one component needs an upgrade, it is an indication that newer technology has arrived and other components likely need upgrading also. Specific considerations of the same four critical areas listed above follows:

- **CPU(s).** If the CPU is causing the bottleneck, it may be more appropriate to replace the entire system than to upgrade. A CPU upgrade would make sense when upgrading from a CPU at the bottom speed of a family to one nearly the top speed of the same family.

- **Memory.** If memory is the bottleneck, upgrading RAM is usually more advantageous than replacing the entire system. However, ensure that enough disk space is available for a larger paging file.

- **Mass Storage.** It is more common to upgrade hard drives than to replace the entire system. The exception to this is when no spare parts are available or if it appears replacement of the entire drive system is needed.

- **Network Connectivity.** Most network components will be easier to upgrade than replace. Network cards, for example, are expansion cards, and a simple matter to swap them out and replace the driver. Replacing network components are required if a system cannot accommodate an upgrade. For example, if a system cannot handle a PCI network card, it will not be able to participate in faster networks such as 100 MB and 1 GB Ethernet, FDDI, or ATM. [Ref. 21]

c. System Roles

Windows 2000 offers much in the way of versatility, having the ability to serve several significantly different roles. Each server role demands a unique configuration, thus demanding different hardware requirements. Depending on the server's role, each system component has a different level of importance. A generalized list of each component's importance to each role is illustrated in Table 4.2.

System Role	CPU	Memory	Mass Storage	Network
Domain Controller	2	1	3	1
File/Print	3	2	1	2
Database	2	2	1	2
Web/FTP	3*	2	3	1
Graphics/Encryption	1	2	3	3

1 = critical, 2 = important, 3 = unimportant
* = If a Web server processes pages prior to transmission (as with .ASP files), the CPU will be important, and in some cases, critical.

Table 4.2. Component Importance for System Roles. After Ref. [21]

C. DEPLOYING WINDOWS 2000

After careful planning, researching the new features and technologies offered, restructuring the domain(s), upgrading hardware, and testing the network is completed, the next step is the actual deployment of the Windows 2000 Server operating system. The section will be limited to the new installation (for example, a new computer with no operating system installed from the factory) of Windows 2000, the upgrade procedure

from an existing Windows NT 3.51-4.0 domain to Windows 2000, and migrating from Novell NetWare to Windows 2000.

1. Upgrade Paths for Windows 2000

Microsoft has put forth much energy to make the Windows 2000 installation process as straightforward and automated as possible. The entire upgrade process is designed to take advantage of Microsoft's standard Setup Wizard utility. The following Microsoft operating systems can be upgraded to Windows 2000:

- Windows 95
- Windows 98
- Windows NT 3.51 (with Service Pack 5 installed)
- Windows NT 4.0

Also, the following restrictions apply to specific Windows NT servers functioning as a PDC, BDC, or member server:

Previous Version	**Upgrade to...**
Windows NT 3.51 or 4.0 PDC	Windows 2000 Domain Controller
Windows NT 3.51 or 4.0 BDC	Windows 2000 Member Server or Windows 2000 Domain Controller
Windows NT 3.51 or 4.0 Member Server	Windows 2000 Member Server. [Ref. 21]

Older operating systems, such as Windows NT 3.1 and Windows for Workgroups 3.11 will require either an upgrade to one of the systems listed above or a new installation.

2. Single Machine Installation

To begin the installation process, the Windows 2000 Setup Wizard must be started. The simplest way to do this is to put the CD-ROM into the CD drive and wait for the prompt. If this is the first operating system to be installed, you may have to boot from the floppy disks, though most new computers allow booting from CD-ROM. If MS-DOS, Windows 3.1, or Windows for Workgroups 3.11 is already installed, the **winnt.exe** command line utility is an alternative. Use the **winnt32.exe** command line utility if Windows 95/98, Windows NT 3.51, or Windows NT 4.0 is installed. Both of these commands will start the Setup Wizard.

a. Setup Wizard Stages

Setup Wizard is designed to guide the administrator through the Windows 2000 upgrade process. This occurs in the four stages listed below. [Ref. 21]:

(1) Stage 1: The Initial GUI Mode Phase of Setup. This is the initial setup screen that appears when the Setup Wizard is launched for the first time. Several key pieces of information are needed to complete this stage. The following items are needed:

- **Licensing Agreement.** A license agreement is needed for each instance of Windows 2000 installed.

- **Regional Settings.** Default settings are English language and the United States.

- **Computer Name and Administrator Password.** Both can be changed after set has completed. Setting an administrator password now will keep the network from being vulnerable to attack as soon as it comes online.

- **Date and Time Settings.** Choose the appropriate time zone and set the correct time.

- **Network Settings.** Select the default settings if DHCP is being used, and network settings will be automatically configured. Manual settings require at a minimum an IP address, subnet mask, and default gateway. DNS and WINS servers can also be specified at this time.

- **Domain Settings.** A user account with the rights to create a computer account in the domain is required for this step. (Normally an administrator handles this installation, so the user account is valid.)

- **Upgrade to NTFS.** If dual-booting with another operating system is not required, upgrading to NTFS at this stage is recommended. Note that NTFS is not optional for domain controllers - it is strictly required to support the Windows 2000 system volume (The actual conversion takes place in Stage 2). However, an existing FAT partition will not be converted to NTFS, even if it is the system or boot partition.

- **Name and Organization.** Self explanatory.

- **Provide Upgrade Packs.** Upgrade packs are used to modify applications to work with Windows 2000. ISVs should make these available if they are necessary. [Ref. 8]

(2) Stage 2: The Initial Text Mode Phase of Setup. After the initial GUI stage is complete it automatically reboots the server. Once back online, it reads the default entry in its BOOT.INI file and begins the initial text mode phase of setup. Windows 2000 loads several files such as NTLDR, NTDETECT.COM, and NTOSKRNL.EXE. These files allow it to initialize essential file systems, drivers, and other devices. NTFS version 4.0 partitions are now converted to NTFS version 5.0

without warning. The conversion includes all logical drives formatted with NTFS version 4.0 also.

(3) Stage 3: The Primary Phase of Text Mode Setup. After an another automatic server reboot the primary phase of text mode setup begins. The core files required to install Windows 2000 are copied from the CD-ROM to the server. After the files are copied, the server's configuration is initialized and saved. The Setup Wizard then reboots the server for the third time.

(4) Stage 4: The Primary Phase of GUI Mode Setup. Windows 2000 loads into GUI mode for the first time in Stage 4. The Setup Wizard launches automatically, then installs and detects various devices, networking components, and other components required by the operating system. The Setup Wizard then creates the Start Menu, registers components, save settings, and removes temporary files used in the upgrade process. A final reboot is required before the Windows 2000 upgrade is complete and ready to be put into service.

3. Deploying Large Sites

While a manual installation for one client machine or up to 20 client machines may be efficient, this would be too cumbersome a task for a large deployment. If a network has more than 15-20 machines that will have a client operating system installed, it would be worth the time and effort to automate the process. Windows 2000 provides two methods of automating installation: the unattended answer file and the Remote Installation Service (RIS).

a. The Answer File

The unattended answer file is a command line parameter used with the Winnt.exe or Winnt32.exe setup file. The answer file is used to bypass the interactive questions asked during Stage 1 of the Setup Wizard (see Chapter IV section 2.a) and can be used to automate the setup process completely. The following is a general description of the answer file as it is used in Windows 2000. A more detailed description can be found in the *Microsoft Windows 2000 Server Resource Kit* (Microsoft Press, 1999).

The format of the unattended setup command line is as follows:

Winnt32 /unattend:<answer file> /s:<install source> [/syspart:<target drive>]

- **/unattend:** In Windows 2000 this parameter specifies the location of the answer file. You can also specify the amount of time Windows NT Setup waits at the boot menu before continuing.

- **/syspart:** In Windows 2000, this parameter causes Windows NT Setup to copy all files for boot and temporary files to the drive and mark it as active. This parameter can only be used with the Winnt32.exe command and is useful if the drive will be duplicated and inserted into other computers as the primary drive.

- **<answer file>:** This file contains the answers to the questions mentioned above in Stage 1 of the Setup Wizard (also known as Unattend.txt in Windows NT 4.0).

In general, an answer file consists of section headers, parameters, and values for those parameters. For example, the different names for 40 computers would be values for the computer name parameter. It is not necessary to specify all the possible parameters or keys in the answer file if the installation does not require it. [Ref. 24]

b. The Remote Installation Service

Remote Installation Service (RIS) is a component of Windows 2000 Server that allows client's systems (for example, Windows 2000 Professional or Windows NT 4.0 Workstation) to be installed with as little administrator interaction as possible. Administrators can power on and boot desktop systems without an operating system installed. To use RIS, several components must be running on the network:

- **DHCP Servers** - Provide the client an IP address as it starts to boot.
- **DNS Servers** - Used to locate the Active Directory servers on the network.
- **Active Directory Servers** - Contain the information about RIS on the network.
- **RIS Servers** - Store the information about the operating system required for the client to boot. [Ref. 8]

During installation, the RIS asks for the location of any operating system installation files. It copies those files from the source (such as a CD-ROM) to a location on the RIS server, which can be used as a network share. These files are then used for client installations.

Windows 2000 RIS is a *boot server*, a server that responds to client requests for boot images. RIS works with clients supporting Pre-Boot Execution Environment (PXE) architecture. When the PXE client boots, it receives two IP addresses form the DHCP server: one for itself, and another indicating its boot server. The client then uses Trivial File Transfer Protocol (TFTP) to download the boot image.

A PXE client will see a customized welcome screen the first time it is started. The client must then log on, after which an installation menu called *OSChooser* will run. This menu is automated by RIS after evaluating which options the user should have access to based on permissions. A user with full permissions will see four options:

- **Automatically setup this computer** - Automatically shows the name and description of any operating system installations the administrator has made available. Multiple installation choices can be offered by the use of several unattended installation scripts, each meeting separate requirements.
- **Customize the setup of this computer** - Gives the client more control over the installation process.
- **Restart a previous setup attempt** - Choose this option if a previous installation failed.
- **Maintenance and troubleshooting tools** - Used to call programs that are outside the standard setup procedure. ISVs and OEMs will provide tools to troubleshoot and update client computers. [Ref. 21]

4. Migrating to Windows 2000

Most Windows 2000 deployments will be upgrades from an older version of Windows operating systems, most likely Windows NT 4.0. However, as the many Novell Netware systems get older, many of these networks will also migrate to Windows 2000. This section explores the entire migration process, breaking it down into six phases: Streamlining, Updating, Planning, Testing, Deploying, and Determining Success or Failure. This section will also look at Migrating to Windows 2000 from Novell NetWare.

a. The Migration Process

The migration process can be very demanding, requiring detailed planning and extensive knowledge of the existing network. These six phases, while similar to the planning required for restructuring domains (introduced in Chapter IV, section 2.a), these phases explore the migration of the operating system at the core of the network. The phases are as follows:

- **Phase One: Streamlining.** Cleaning up the existing network is a good idea anytime, but it is especially beneficial to do this before upgrading the network and servers. Some objects to concentrate on are:
  - Audit the user account database for duplicate or unused accounts.
  - Clean unnecessary files off all servers and desktop systems, and ensure all systems have ample free space.
  - Perform any hardware upgrades needed to bring the network up to Windows 2000 standards.
- **Phase Two: Updating.** Many of the new features built into Windows 2000 operating system have been released as add-ons. For example, the Microsoft Management Console and Dynamic Domain Name Service (both introduced in Chapter 3) can be integrated in a Windows NT 4.0 network. Make sure that the TCP/IP services included with Windows NT 4.0 are being implemented. This includes implementing WINS, DNS, and DHCP.
- **Phase Three: Planning.** Planning involves several important tasks before upgrading the operating system.
  - Create a diagram of the new architecture and document any hardware or software needed for the migration.
  - Specify a budget for the deployment. Be sure to include hardware and software upgrades, new hardware, and personnel costs.

- Create a detailed list specifying every task that is required for the migration. This should include all hardware and software upgrades, synchronization of domain controllers, backups, and when to inform users that specific servers will be offline.

- Specify a timeline when tasks will be completed, and schedule tasks that can be completed simultaneously to occur.

- **Phase Four: Testing.** Build a small testing lab in which Windows 2000 is loaded along with other network applications. Ensure that all applications work as it did prior to the upgrade.

- **Phase Five: Deploying.** Small networks (50 clients or less) can usually migrate in one step. Larger organizations may want to migrate in phases, such as migrating PDCs, then BDCs, leaving a one week interval to ensure the migration was successful. The last step is to migrate client systems one department at a time.

- **Phase Six: Determining Success or Failure.** After the migration is complete, conduct a series of tests to validate functionality. Support issues will arise, but with proper planning and documentation, can be dealt with in a reasonable timeframe. [Ref. 8]

Finally, a migration to Windows 2000 is a task not to be taken lightly. It will require teamwork, planning, a system to track completed tasks, and possibly a project manager to lead the migration team. A good knowledge of the Windows 2000 operating system and the network is essential to a successful migration.

b. Migrating to Windows 2000 from Novell NetWare

Windows 2000 includes, not surprisingly, a hearty tool to help migrate resources from Novell NetWare. The Directory Services Migration Tool allows you to migrate Bindery and Novell Directory Services (NDS) objects, as well as volumes from NetWare, to Windows 2000 and Active Directory. The Directory Services Migration

Tool supports migrating from NetWare 3.x, 4.x, and 5.0. The migration involves three general steps:

- **Creating and Modeling a View from NetWare.** Collect information from the Bindery or from NDS (Netware 3.x support Bindery operations, while Netware 4.x or later support NDS). This includes network objects such as users, groups, and organizational units.

  - Launch the Directory Services Migration Tool, then create a new project to house the view from NetWare. Next, create the View of the NetWare NDS Tree.

  - Modify any object in the View before beginning the migration. For example, objects can be created, deleted, and moved in the modeling phase, and users can be added to groups or set options for creating new passwords.

- **Configuring a View to Active Directory.** This step involves configuring the View to Active Directory. Each object in the View is copied to the Active Directory. Once each object is created in Active Directory and verified, exit the Directory Migration Services Tool.

  - Launch the Windows 2000 Directory Management Tool to verify each object was created successfully in the Active Directory.

  - Be aware of the differences between NetWare NDS and Windows 2000 Active Directory. NDS uses rights while Active Directory uses permissions. The migration from rights to permissions follows a set of rules and is automatically mapped from NDS to Active Directory.

- **Migrating NetWare Volumes to Windows 2000.** The Directory Migration Services Tool can be used to migrate files and their security attributes, and volume objects, from NetWare to Windows 2000.

  - Select a volume object in the NetWare View and launch the File Migrate Wizard from the drop-down context menu.

  - Decide whether or not to migrate security attributes from the NetWare volume.

  - Choose whether or not to migrate selected files from the NetWare volume.

- Specify the drive on the Windows 2000 server where the NetWare volume will be stored.

- Review the permissions that will be assigned to NetWare files that will be migrated.

- The File Migrate Wizard creates the new share on the Windows 2000 server. After the share is created, the wizard completes the migration of the NetWare volume and all permissions. [Ref. 23]

Finally, after migrating the NetWare volumes and permissions to Windows 2000, the NetWare server can be decommissioned. NetWare users can now access the same resources in which they previously had access to on the newly created share on the Windows 2000 server.

D. CHAPTER SUMMARY

Preparing a network for Windows 2000 is as important, if not more, than the actual deployment of the operating system itself. Careful planning will prepare you for any problems that may arise during the migration process. A thorough study of the existing domain(s) will aid in deciding when to restructure the domain(s) - before or after the upgrade. A thorough understanding of Active Directory is also required before any decisions concerning restructuring a domain for the migration to Active Directory can be made. Understanding how Trees, Forests, Organizational Units, and Sites make up the Active Directory will simplify all phases of the migration process. Finally, thorough knowledge of the deployment process will ensure that the migration to Windows 2000 will be successful with as few problems as possible.

V. WINDOWS 2000 SECURITY FEATURES

Microsoft Windows 2000 Server provides a robust and sophisticated standards-based network security system. Two technology areas that are growing rapidly to meet higher-level security needs in today's increasingly complex networking environments are public-key certificates and dynamic passwords. At the heart of Windows 2000 security is the Distributed Security Services, a new set of services made up of many new features that take advantage of these swiftly changing security technologies. This chapter discusses the security features offered by Windows 2000 and how new security technologies are implemented to provide state-of-the-art network security.

There are numerous areas in which Windows 2000 security is adapting to support the Internet-based enterprise. Some of these adaptations indicate advances in supporting large organizations through the use of Active Directory, while other changes take advantage of the flexibility of the Windows 2000 security architecture. The Windows 2000 security architecture is specifically designed to incorporate new security technology in the form of protocols, cryptographic service providers, and third party authentication technology. To meet the fast-changing technologies and growing demands of users, Microsoft developed the Distributed Security Services for Windows 2000. Distributed security is security in which the participants are not part of the same network and have no common security credentials. The Distributed Security Services is a feature of Windows 2000 that integrates established Internet standards for authentication while simultaneously

introducing new public-key security technology. It has many new features to simplify domain administration, improve performance, and integrate new technologies based on public-key cryptography. Highlights of the Windows 2000 Distributed Security Services include:

- Integration with Windows 2000 Active Directory to provide scalable, flexible account management for large domains with fine-grain access control and delegation of administration.
- Implementation of the Kerberos version 5 authentication protocol to provide a foundation for authentication interoperability.
- Strong authentication using public-key certificates, secure channels based on Secure Sockets Layer (SSL) 3.0, and CryptoAPI to deliver industry-standard protocols for data integrity and privacy across networks. [Ref. 26]

Windows 2000 Distributed Security Services is a set of applications and technologies for administrators to use in developing a security plan. The remainder of this chapter discusses the technologies and features of Windows 2000 security.

A. ACTIVE DIRECTORY AND SECURITY

Windows NT 3.x-4.0 account information is maintained using a secure portion of the registry on domain controllers. These accounts are maintained in a flat-namespace with no internal organization. Windows 2000 Distributed Security Services uses the Active Directory as the storage area for account information, a great improvement over the registry-based implementation used in Windows NT 3.x-4.0. Figure 5.1 illustrates the

structure of Windows 2000 domains, and the hierarchical name context within each domain using Organizational Units (OUs) as directory object containers.

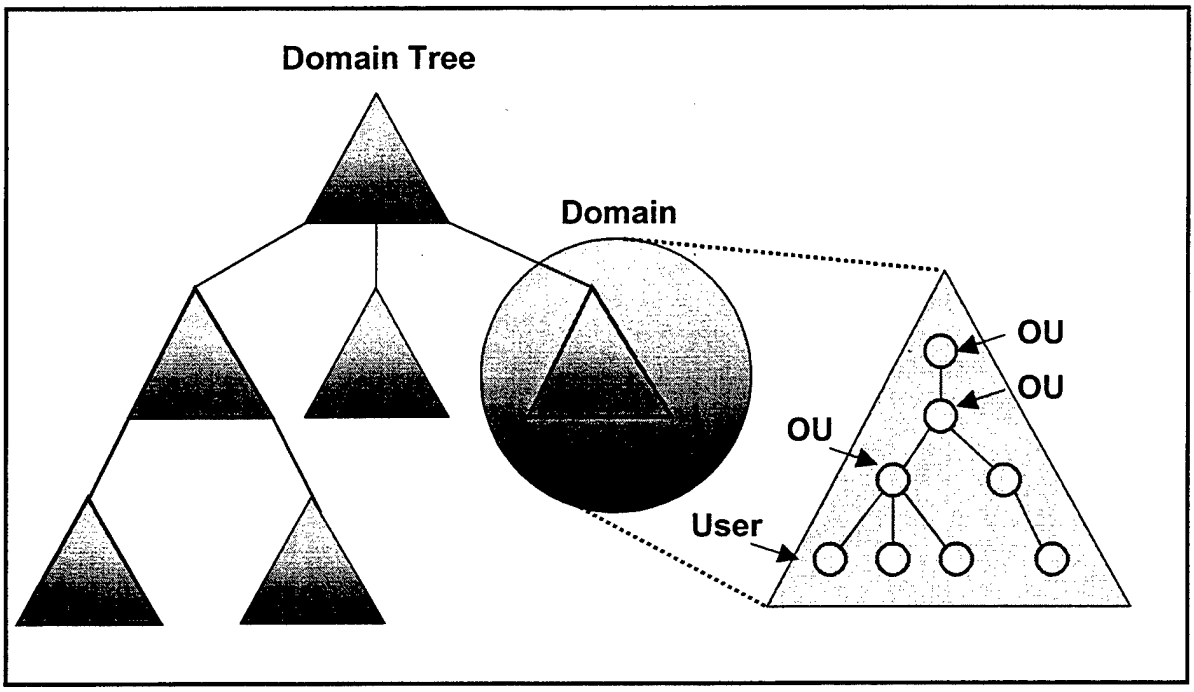


Figure 5.1. Hierarchical structure of the Active Directory. After Ref. [26]

There are several advantages of integrating security account management with the Active Directory. They include:

- Users, groups, and machine accounts can be organized into directory containers, or OUs. This allows administration in a hierarchical, tree-structured namespace rather than a flat namespace.

- Active Directory supports over one million user objects with better performance than the registry, eliminating the limits imposed by the Security Accounts Manager (SAM) database in Windows NT 3.x-4.0 domains.

- Graphic tools available in Active Directory management can also be used to administer account information. [Ref. 26]

Storing the SAM database in Active Directory ensures that users and groups are represented as objects in the directory. Read and write access to objects in the directory can then be granted to the object as a whole, or to individual properties of the object. Administrators are also given fine-grain control over who can update user or group information. For example, a graphics group can be granted write access only to user account properties related to graphic printers without requiring full Account Operator or Administrator privileges.

1. Active Directory and Security Services

There is a fundamental relationship between the Active Directory and the Security Services integrated into the Windows 2000 operating system, as illustrated in Figure 5.2. Active Directory stores the domain security policy information. This includes the domain-wide password restrictions, system access privileges, and the SAM database. Security-related objects in Active Directory require secure management to avoid unauthorized changes that could affect overall system security. Windows 2000 implements an object-based security model and access control for all objects in the Active Directory. Every object in the Active Directory has a unique security descriptor that defines access permissions that are required to read or update the object properties. [Ref. 26]

The Windows 2000 security model provides a unified and consistent implementation of access control to all domain resources that is based on group

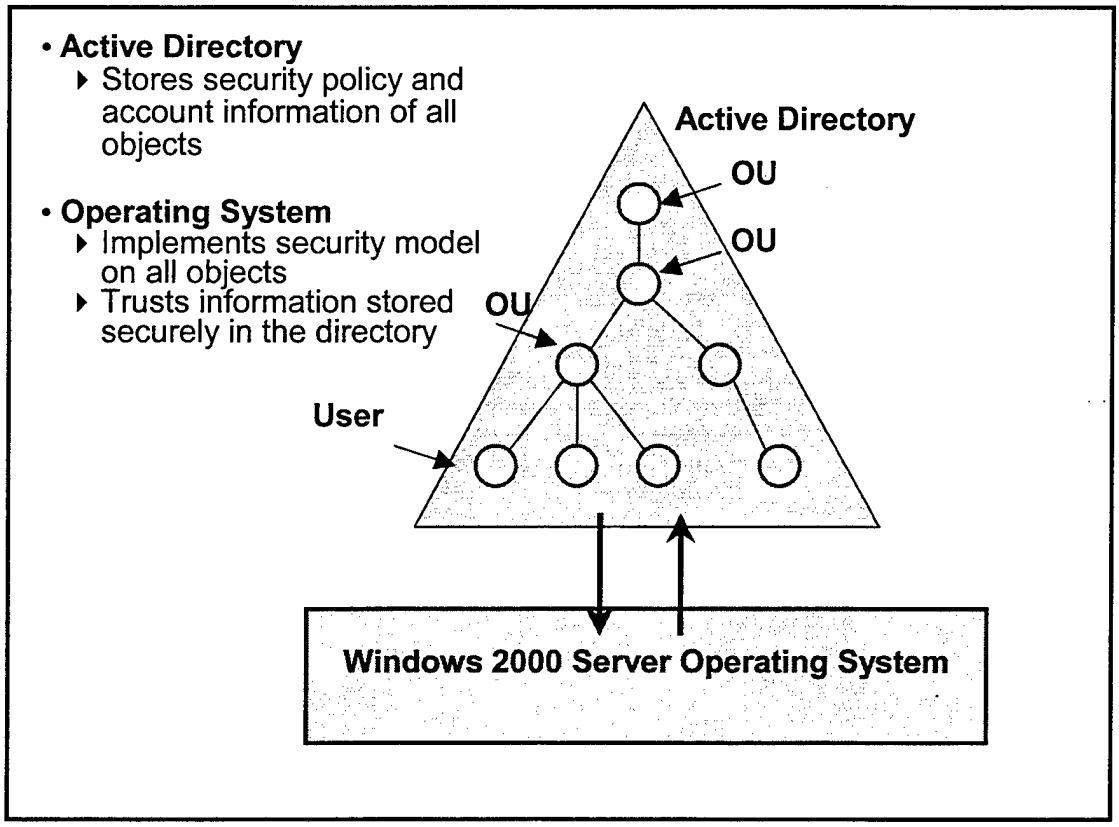


Figure 5.2. Relationship Between the Active Directory and Security Services. After Ref. [26]

membership. Active Directory does not make access-control decisions; rather, it requires the Windows 2000 operating system to enforce access control.

The Windows 2000 security components can trust the security-related information stored in Active Directory. For example, the Windows 2000 authentication service stores encrypted password information in a secure portion of the user objects in Active Directory. The operating system trusts that security policy information is securely stored and account restrictions or group membership is not changed without authorization. The security policy information for overall domain management is also kept in a secure

portion of Active Directory. This fundamental relationship between Active Directory and Security Services is only achieved by complete integration of Active Directory with the Windows 2000 operating system. [Ref. 26]

2. Securing Active Directory

To successfully implement Active Directory, an administrator must first understand Microsoft's philosophy behind Windows 2000 distributed security. This philosophy is as follows:

- Assign access rights as high up as possible in the OU tree. This achieves the maximum effect with minimum effort. Ensure that the access rights are suitable to the underlying objects.
- Use inheritance to spread access rights into the OU tree. All objects under a particular object immediately inherit that object's assigned rights.
- Administer the rights to users through groups. Permissions assigned at the user level are difficult to track and manage. You can create a hierarchy of group objects before creating the first user. [Ref. 1]

Active Directory enables an administrator to delegate rights efficiently and flexibly, and is a valuable tool with which to confine the security administration to a well-defined subset of users in an organization. An administrator should allocate rights to administer a small set of users or groups to relevant members and withhold permissions to manage accounts in other parts of the organization.

Delegation of responsibility to create new users or groups is defined at the OU level, or container, where the accounts are created. Group administrators from one OU will not necessarily have the ability to create and manage accounts for other OUs within a

domain. However, domain-wide policy settings and access rights defined on a higher level in the directory tree may cover the entire tree through inheritance of access rights.

Active Directory uses three methods to define delegation of administration responsibilities:

- Delegate permissions to change properties on a particular container at the OU level. Delegating routine tasks at the OU level facilitates the formation of an administrative model that is both efficient and easy to manage.
- Delegate permissions to create and delete child objects of a specific type beneath an OU, such as users, groups, or printers.
- Delegate permissions to update specific properties on child objects of a specific type beneath an OU; for example, the right to Set Password on User Objects. [Ref. 26]

There are some difficulties involved with administering security through Active Directory. First, you cannot administer users based on their location in the Active Directory hierarchy. This must be done through groups. However, Microsoft has introduced a hierarchy in Active Directory in which groups can be embedded within other groups, which simplifies administration. Second, administrative rights cannot cover multiple domains through trust relations, constraining Active Directory to be administered as a series of independent domains, not as one continuous directory tree. This applies to resources as well, as resource access control lists (ACLs) cannot be spread over multiple domains.

3. Security Tools

Microsoft has designed a set of MMC Snap-ins to answer the need for a central security configuration tool. The Security Configuration Tool Set is designed to reduce security-related administration costs by defining a single point where the entire system's security can be viewed, analyzed, and adjusted. The tool set allows the administrator to define a number of configuration settings and have them implemented in the background. Configuration tasks can also be grouped and automated, simplifying the task of configuring a group of computers.

The Security Configuration Tool Set will complement existing system security tools (such as User Manager, Server Manager, and Access Control List Editor), not replace them. Its goal is to complement existing tools by defining an engine that can interpret a standard configuration file and perform the required operations in the background.

The Security Configuration Tool Set consists of the following Snap-ins:

- **Security Configuration Service** - The core engine of the Security Configuration Tool Set. It runs on every Windows 2000-based system and is responsible for all security configuration and analysis functionality provided by the tool set. This service is central to the entire network infrastructure.

- **Setup Security** - Creates the initial security database, called the *Local Computer Policy* database, on every computer with a clean installation of Windows 2000.

- **Security Configuration Editor** - Allows administrators to define computer-independent security configurations in a template and save it as a text file.

- **Security Configurations Manager** - Allows administrators to import security templates defined by the Security Configuration Editor to a security database.

This builds a machine-specific security database, which stores a composite configuration.

- **Security Settings Extensions to the Group Policy Editor -** Extends the Group Policy Editor, allowing administrators to define security configuration as part of a group policy object. Group policy objects can then be assigned to a specific computer, domain, or OU scope in the Active Directory. [Ref. 27]

B. THE KERBEROS AUTHENTICATION PROTOCOL

Windows 2000 supports several core authentication protocols: Windows NT LAN Manager (NTLM), Secure Sockets Layer (SSL), Distributed Password Authentication (DPA) and Kerberos. NTLM is used by Windows NT 3.x-4.0 (downlevel domains) and remains largely proprietary. Kerberos replaces NTLM as the primary security protocol for access to resources within or across Windows 2000 domains and is probably the most important security component in a Windows 2000-based network. It offers a three-sided authentication process, with shared-secret keys that enable users to prove their identity. This section introduces the Kerberos authentication protocol and how it is implemented in Windows 2000 Security Services.

1. Understanding the Kerberos Authentication Protocol

Kerberos is an Internet standard for authentication and defines the interactions between a client and a network authentication service. The Windows 2000 implementation of a network authentication service is known as a Key Distribution Center (KDC). The Kerberos protocol is based upon the KDC and *tickets.* Tickets are encrypted data packets issued by the KDC. A ticket vouches for a user's identity as well

as carrying other information. A KDC provides tickets for all users within its area of authority (normally a domain, or what Kerberos calls a *Realm*). Every domain controller in Windows 2000 is a KDC. [Ref. 26]

The Kerberos authentication protocol augments the built-in security features of Windows 2000 with the following enhancements:

- Faster server authentication performance during initial connection establishment. The application server does not have to connect to the domain controller to authenticate the client, allowing application servers to better handle large numbers of client connection requests.

- Delegation of authentication for multitier client/server application architectures. When a client connects to a server, the server impersonates the client on that system. But if the server needs to make a network connection to complete the client transaction, Kerberos allows delegation of authentication for the first server to connect on the client's behalf to another server, and allows the second server to also impersonate the client.

- Transitive trust relationships for interdomain authentication. Users can authenticate to domains anywhere in the domain tree because the KDCs in each domain trusts tickets issued by other KDCs in the tree. Transitive trust simplifies domain management for large networks (as explained in Chapter III). [Ref. 27]

2. Authentication Using the Kerberos Protocol

The Kerberos protocol defines a series of exchanges between clients, the KDC, and servers to obtain and use Kerberos tickets. Kerberos security is based on two fundamental concepts:

- **Shared Keys** - The user and the KDC share the same secret key (normally the user's password).

- **Three-sided Authentication** - The authentication process involves three components:

- The *client*, which represents the user.
- The *resource* that wants to ensure the client is legitimate, often a server.
- A *KDC*, which serves as a central repository for client information. [Ref. 1]

Kerberos is a shared-secret authentication protocol because both the user and the KDC know the user's password. An illustration of how Kerberos is used in authenticating users in Windows 2000 is provided in Figure 5.3. When a user initiates a logon to Windows 2000, the user authenticates to a KDC. The KDC provides the user with an initial ticket called a Ticket Granting Ticket (TGT). Windows 2000 stores the TGT in a ticket cache on the workstation associated with the user's logon context. When the user needs to use a network resource, his user session presents the TGT to the domain controller and requests a ticket for the particular resource. This ticket is called a Service Ticket (ST). The user then presents the ST to the resource, which grants him access. [Ref. 28]

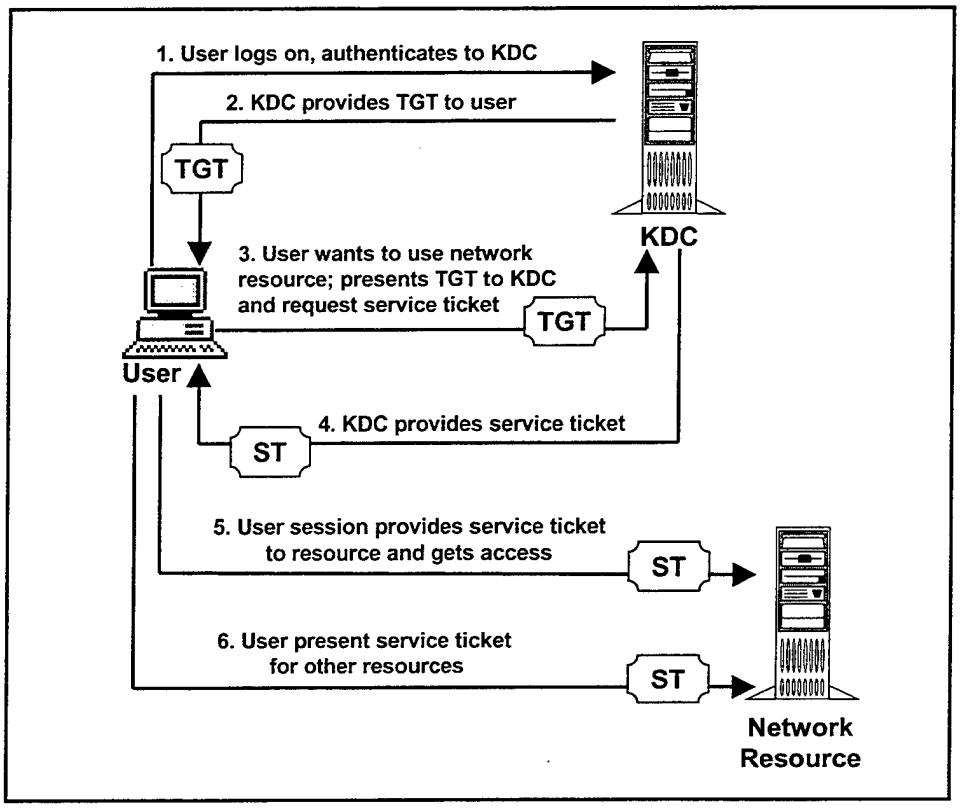

1. User logs on, authenticates to KDC
2. KDC provides TGT to user
TGT
KDC
3. User wants to use network resource; presents TGT to KDC and request service ticket
TGT
User
4. KDC provides service ticket
ST
5. User session provides service ticket to resource and gets access
ST
6. User present service ticket for other resources
ST
Network Resource

Figure 5.3. Authentication using the Kerberos Protocol. After Ref. [28]

3. Improved Network Performance

The Kerberos protocol is fully integrated with the Windows 2000 security architecture for authentication and access control. In fact, it is the default authentication method. In most network authentication protocols (including NTLM), the network's security authority must provide authentication for every use of a network resource. For example, in a Windows NT 4.0 domain, a domain controller has to vouch for a client's identity every time he needs to use a network printer, even if it was the same printer the client had used minutes before.

Kerberos removes this bottleneck by issuing a ticket to authenticated users. A domain controller 's sole participation in a client's use of a resource is to issue the ticket to the user's session. Once a ticket has been issued, the domain controller is no longer involved and the client can present his ticket as many times as necessary for use of that specific resource. Tickets are stored in a local cache (which is part of the security architecture's protected storage), and when one is needed, the user's session retrieves the ticket from the cache and presents it to the resource. Tickets are reusable and remain so until they expire. The lifetime of a Kerberos ticket is set in accordance with the security policy and is normally set to 8 hours. [Ref. 28]

4. Single Sign-on in Windows 2000 Networks

Single Sign-on (SSO) allows enterprise network users to seamlessly access all authorized network resources on the basis of a single authentication process. SSO is the ability of a user to prove his identity (that is, to authenticate himself) to a network one time, and from that point on have access to all authorized network resources without additional authentication. SSO is provided natively in Windows 2000 domains by the built-in Kerberos authentication protocol.

The greatest benefits of SSO are obtained from implementing Windows 2000 homogenous domains, but significant benefits can be found even when deploying Windows 2000 in heterogeneous networks. One such benefit is that since SSO for Windows 2000 interoperates with numerous operating systems, it is an ideal choice to serve as an SSO hub in heterogeneous networks. Other benefits include:

- **Simpler administration.** SSO for Windows 2000 uses the same administration tools for SSO-specific tasks an administrator uses for other administrative tasks.

- **Better administrative control.** All network management information, including SSO-specific information, is stored in the Active Directory, producing a single authoritative list listing of each user's rights and privileges. Any changes made to a user's account will propagate through the entire network.

- **Improved user productivity.** Clients no longer have to use multiple logons or multiple passwords in order to access network resources.

- **Better network security.** All SSO methods available under Windows 2000 provide secure authentication and provide a basis for encrypting the user's session with the network resource. Network security is enhanced because of the consolidation of network management information in the Active Directory. When an administrator disables a user's account, the administrator knows with certainty that the account is fully disabled.

- **Consolidation with heterogeneous networks.** Joining other dissimilar networks, allowing a central administrative focal point for security policies to be enforced can consolidate administrative efforts. [Ref. 28]

5. Kerberos Weaknesses

To some degree, all networked systems are susceptible to some type of computer attack, unauthorized access, or computer fraud. While Kerberos is the most optimal solution to securing distributed networks, it does have weaknesses.

The most obvious risk to Kerberos is from a dictionary attack on passwords. A dictionary attack is one where commonly used passwords are compared against a password or password file to gain unauthorized access. While a strict and effective

security policy will offset this weakness, Kerberos still remains susceptible, and Windows 2000 security facilities do not currently offer an adequate solution.

Another weakness is that the KDC must be physically secured. An unauthorized user who gains access to the KDC could potentially gain unrestricted access to the entire network.

Possibly the most difficult risk to offset is the human factor. It is virtually impossible to stop trusted staff members or administrators from accessing applications or files in which they have no need to know, but because of the nature of their job, they must have access to properly administer the system. In a case such as this, no security system is able to provide the needed protection.

With these weaknesses in mind, remember that Kerberos is currently the best solution for a secure and easily administered security-authentication system for distributed networks. Kerberos gives clients proof that a server is what it claims to be, and introduces a time limit (by way of a ticket's lifetime) in the client's access to servers and resources across a network. Kerberos can easily be used to handle more domains and is swiftly becoming the standard for authentication access control. [Ref. 1]

C. INTERNET SECURITY AND PUBLIC-KEY INFRASTRUCTURE

Microsoft is developing a public-key security infrastructure to be integrated with Windows 2000 security. Public key cryptography is the security technology that enables strong security for enterprise and Internet communications. When properly implemented public-key cryptography offers significant security benefits. However, it requires an

infrastructure to deliver its benefits. The Windows 2000 operating system includes a native public-key infrastructure (PKI) that is designed to take full advantage of the Windows 2000 security architecture. While other studies have focused specifically on Internet security or PKI, this section will be limited to describing the features and benefits provided by the native PKI designed in the Windows 2000 operating system. [Ref. 29]

1. Overview of Public-key Cryptography and PKI

The purpose of PKI is to make the implementation of public-key cryptography as easy as possible. Public-key cryptography is essential for Internet, intranet, and other applications that require distributed security. Public-key cryptography provides three important capabilities for businesses and organizations:

- **Privacy** - Public-key cryptography provides privacy via data encryption. For example, encrypting e-mails sent across the Internet, preventing them from being read, and encrypting network traffic when users visit a website.

- **Authentication** - Identification of users and resources. For example, verifying the identity of a visitor to an intranet in order to allow them to read certain files.

- **Non-Repudiation** - The ability to prove that someone took a particular action. For example, the ability to create an enforceable, tamperproof, record of a user's actions concerning sensitive files. [Ref. 29]

Public-key systems use two keys: a public key, designed to be shared, and a private key, which must be closely held. These keys work together to provide secure communications: if you encrypt something with a public key, it can only be decrypted with the corresponding private key, and vice versa. An often-used example of the public-

key cryptography is illustrated in Figure 5.4 by two well-known computer users -- Bob and Alice. If Bob wants to send Alice a secret message, he uses her public key to encrypt it, then sends it to her. Once Alice receives the encrypted data, she uses her private key to decrypt it. The concept is that public keys can be freely distributed so others can use it to encrypt data to send to you that only you can decrypt with your private key.

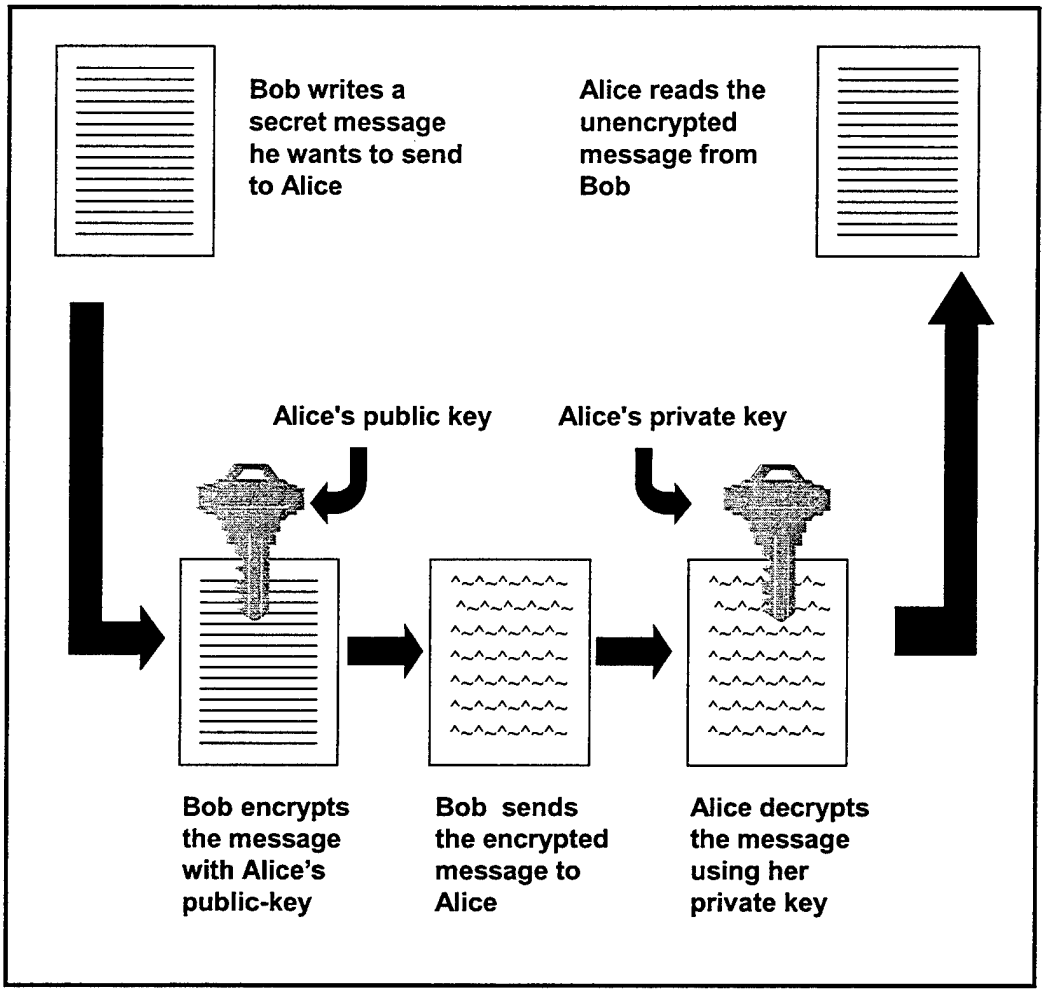

Bob writes a secret message he wants to send to Alice
Alice reads the unencrypted message from Bob
Alice's public key
Alice's private key
Bob encrypts the message with Alice's public-key
Bob sends the encrypted message to Alice
Alice decrypts the message using her private key

Figure 5.4. Encryption Using the Public Key System.

A PKI is not a physical object or a software process; it is a set of operating system and application services that make it easy and convenient to use public-key cryptography. A PKI provides a system with the following capabilities:

- **Manage keys** - A PKI makes is easy to issue new keys, review or revoke existing keys, and manage the trust level attached to keys from different issuers. Windows 2000 uses Certificate Server (included in IIS 4.0) to provide key management.

- **Publish keys** - A PKI offers a well-defined way for clients to locate and retrieve public keys and information about whether a specific key is valid or not. Without the ability to retrieve keys and know that they are valid, clients cannot make use of public key services.

- **Use keys** - A PKI provides an easy-to-use way for clients to use keys by providing applications that perform public-key cryptographic operation, making it possible to provide security for e-mail, e-commerce, and networks. [Ref. 29]

Public keys are objects that a PKI uses. While public keys are required for PKI-based security, they are usually packaged as digital certificates. The certificate contains the public key and a set of attributes, such as the key holder's name.

2. Windows 2000 PKI

Windows 2000 includes a full-featured PKI that delivers the security benefits of public-key cryptography. Windows 2000 PKI is a built-in feature of the operating system and is seamlessly integrated into normal network management tasks.

The Windows 2000 PKI is built on four basic premises:

- **Interoperability** - The ability to exchange messages, certificates, and services with other standards-based PKI components.

- **Security** - Provided by using robust security algorithms and procedures and by depending on mature, well-tested code and algorithms.

- **Flexibility** - The ability to configure a PKI that matches a specific organizational and administrative needs with minimum amount of hassle.

- **Ease of use** - Easy setup for administrators, and users will find it easy to obtain and use certificates. [Ref. 29]

Windows 2000 PKI is made up of several services that provide Internet security services. The primary components of the Windows 2000 PKI are:

- **Certificate Services** - A core operating system service that allows businesses to act as their own Certificate Authorities and manage digital certificates.

- **Active Directory Service** - A core operating system service that provides a single place to find network resources; it serves as the publication service in the PKI.

- **PKI-enable Applications** - Applications such as Internet Explorer, Microsoft Money, Internet Information Server, Outlook, and Outlook Express, and numerous third-party applications that interoperate with the Windows 2000 PKI.

- **Exchange Key Management Service (KMS)** - A component of Microsoft Exchange that allows for the archiving and retrieval of keys used to encrypt e-mail. [Ref. 29]

Windows 2000 PKI offers robust security to the enterprise environment. All components rely on open industry security standards, ensuring interoperability. Windows 2000 offers an open security that allows third-party applications, including third-party PKIs, to use its robust security features. However, the Windows 2000 PKI provides the best integration with the Active Directory service because it is a built-in component of the operating system.

D. CHAPTER CONCLUSION

Microsoft has endeavored to increase Windows 2000 security facilities over those of past Windows NT operating systems. They have also made them considerably easier for administration and access control. Almost all the security facilities are part of the Security Configuration Tool Set (a set of MMC Snap-in tools), which enables an administer to configure the security for the Windows 2000 environment and carry out periodic analysis of the network's security.

The Windows 2000 Distributed Security Services provides flexible solutions for building secure, scalable distributed applications. Interdomain trust management is simpler, providing greater flexibility and allowing organizations to use domains that more closely reflect the needs of the organization. It integrates Internet standards for authentication (Kerberos) while introducing new public-key security technology. The Windows 2000 security architecture is specifically designed to incorporate new security technology in the form of protocols, cryptographic service providers, or third-party authentication technology.

Windows 2000 Distributed Security Services offers flexibility to administrators in how they integrate security into their application environment, what security technologies to use, and when to implement a new technology. These features and capabilities make the Windows 2000 Distributed Security Services the best foundation for enterprise and Internet-based environments.

VI. CONCLUSION

Any time a new innovation in technology is implemented, questions undoubtedly arise. The Windows 2000 server operating system is no exception to this as many of its new features are built around leading edge technologies. Even though Windows 2000 is the fifth major revision of the Windows NT operating system, it is the first version that implements Active Directory, NTFS 5.0, Internet standards support, Encrypted File system, and many more features.

It is essential for IT directors to carefully review the system requirements, client's needs, and benefits offered by Windows 2000 before actually installing the operating system. Careful planning and a systematic approach to the physical implementation of the operating system and hardware is required for a successful deployment to occur. While central administration, enhanced manageability, and improved security are of great benefit, Windows 2000 remains a complex and daunting environment that requires IT managers to take a slow approach to the deployment process. An in depth understanding of all the issues surrounding a Windows 2000-based network is required, from understanding the hardware requirements to how clients will interact with Active Directory. To ensure your deployment plan works, implementing Windows 2000 in a controlled environment is strongly recommended.

Windows 2000 offers many compelling advantages that provide IT managers an operating system that will meet organizational requirements well into the next

millennium. However, they must be cognizant of operating system updates Microsoft will undoubtedly be required to provide once the operating system is distributed and tested in real world situations. By incorporating the latest technologies, implementing an open architecture, and designing features that will decrease the total cost of ownership to organizations, Microsoft has made assurances that Windows 2000 will be a healthy and useful operating system that will serve the needs of business and organizational clients for years into the future.

APPENDIX A. WINDOWS 2000 IMPROVEMENTS TO WINDOWS NT 4.0

The Windows 2000 Server operating system is not merely an upgrade of Windows NT Server 4.0. It is a completely redesigned system that offers many new features and takes advantage of the latest technologies available. Windows 2000 builds on the strengths of Windows NT Server 4.0 by providing a platform that is faster, more reliable, easier to manage, and built from its inception using the latest industry standards. The following is a detailed list of the key features offered in Windows 2000 Server, along with a comparison of each feature to what is offered by Windows NT server 4.0. The comparison tables are divided into seven categories:

- Table A.1 - Network and Communication Servers
- Table A.2 - File Sharing and Storage Servers
- Table A.3 - Printing and Sharing Services
- Table A.4 - Manageability
- Table A.5 - Security Services
- Table A.6 - Application Services
- Table A.7 - Web Services. [Ref. 30]

Table A.1. Networking and Communication Services. After Ref. [30]

Feature	Windows NT Server 4.0	Windows 2000 Server
TCP/IP	Microsoft has provided a native TCP/IP stack with Windows NT Server since version 3.1. Many performance improvements have been made through product releases.	Windows 2000 Server has been updated for networking within high-bandwidth LAN and WAN environments.
Auto-net Configuration and connection sharing	Not available	For small workgroups, Windows 2000 Server will automatically configure an entire network and connect it to the Internet through a demand-dial router interface by clicking a single check-box. The server automatically defines IP addresses, sets up DHCP and a DNS proxy, and configures the default gateway.
Quality of Service (QoS)	Not available	Managed, end-to-end, express delivery system for IP traffic. Includes Admission Control Services to policy check network resources requests, APIs for creation of QoS aware applications, and end-system policy enforced marking of packets for QoS.
ATM Gigabit support	Available through third parties.	Provides native support for ATM and Gigabit networking.
VPN Support	Microsoft worked as part of a multivendor effort to create Point-to-Point Tunneling Protocol (PPTP) to provide customers with a secure and easy to use VPN solution in Windows NT Server 4.0. As part of Windows NT 4.0, PPTP supports VPN connections client-to-server and server-to-server.	Windows 2000 Server builds on the PPTP support and adds widely used protocols including IPSec and L2TP to enable secure VPN solutions. Customers can choose from these protocols as needed to match against different business requirements. Protocol negotiation and integration within a common interface hides the distinctions from the end-user.

Remote Access Services	Remote Access Services (RAS) provides end-users with direct-dial connections to corporate networks. RAS integrates direct-dial and VPN access within a common service and common user interface. Up to 256 concurrent connections are supported.	Windows 2000 continues the integration of direct-dial and VPN and expands this with choices of VPN protocols and a comprehensive policy management system. Policy can be applied based on the type of connection, the user/group, the time of day, the type of encryption and more to grant or deny access.
RADIUS Support	Part of the dial-up network client allowing authentication into ISP networks or non-Windows corporate direct-dial networks. Support for a RADIUS Server is provided so that ISPs and non-Windows clients can authenticate against the Windows NT Server domain.	Full-fledged RADIUS functionality. Supports both RADIUS authentication RADIUS accounting. Stores information in Active Directory or a local database. Offers an intuitive graphical user interface for the most commonly needed attributes.
Network Address Translator (NAT)	Available by adding Microsoft Proxy Server to a Windows NT 4.0 server.	Network Address Translator (NAT) hides internally managed IP addresses from external networks by translating the private internal addresses to a public external address. Windows 2000 includes a complete address and port translation NAT that supports any IP version 4 client, and includes NAT translation for PPTP based VPN traffic.
Multi-Protocol Routing	Supports: RIP (v1 and v2) for IP and SAP for IPX, Open Shortest Path First (OSPF), DNS Proxy, DHCP Relay Agent, Static Routing, Demand-dial routing, and Bandwidth Allocation Protocol.	Adds Active Directory integration and MMC based management for centralized management of multiple routers. IGMP is also supported to allow multiple to share a single multicast session, reducing traffic through slower branch office router connections.
IP Telephony	Offered through the Telephony Application Program Interface (TAPI). TAPI 2.0 includes call control features that work with a variety of existing telephone switches.	TAPI 3.0 unifies IP and traditional telephony to enable developers to create anew generation of powerful computer telephony applications. Expands call-control capability and supports ITU standards for voice and video over IP networks.

Table A.2. File Sharing and Storage Services. After Ref. [30]

Feature	Windows NT Server 4.0	Windows 2000 Server
Index Services	Available for Web content indexing and searching.	Integrated Indexing services provides users with a fast and easy way to search for information on the network. Search for content on a Web share or file share.
Dynamic Volume Management	Able to extend volume sets, requires server to be rebooted.	Add disk space to NTFS volume without rebooting or interrupting users.
Distributed Link Tracking	Not available.	Resolves shortcuts and links to NTFS-resident files that have undergone a change in name or path.
File Compression.	Built into NTFS, provides seamless file compression services	Same.
Disk Quotas	Available through third party vendors.	Per-user disk quotas to monitor and limit disk space use.
Hierarchical Storage Management	Not available.	Remote Storage Services (RSS) automatically monitors the amount of space available on a local hard disk and removes local data that has been copied to remote storage, freeing up disk space.
Removable Storage Management (RSM)	Not available.	RSM presents a common interface to robotic changers and media libraries, enables multiple applications to share local

Distributed File System (DFS) Support	Shipped as an add-on service. **Fault Tolerance** - In the event that multiple replicated servers make up a DFS share, users are automatically redirected to the servers that are available. This is also true if the server is taken offline during a file operation. **Load Balancing** - Access to DFS shares consisting of multiple servers will be automatically balanced among the available servers.	Provides a single logical view of file shares across multiple servers and different file systems such as NTFS, NetWare, and NFS. **File Replication** - A DFS share can be made up of multiple shares across multiple servers with the same content to provide fault tolerance and load balancing. Windows 2000 includes file replication to keep the content between the shares in sync. **Site Proximity** - Users are automatically redirected to the replicated server/share closest to them, transparent to the users. A DFS share appears as a regular file share to clients.

Table A.3. Printing and Sharing Services. After Ref. [30]

Feature	Windows NT Server 4.0	Windows 2000 Server
Directory Integrated	Not available	Publishing in the Active Directory allows users to quickly locate the most convenient printing resources. Active Directory integration makes all shared printers in a domain available in the directory.
Broad Device Support	Provides support for more than 1,000 different print devices on the CD.	Provides support for more than 2,500 different print devices on the CD.
Internet Printing Protocol (IPP)	Not available.	Lets users print directly to a URL over an intranet or Internet.

Table A.4. Manageability. After Ref. [30]

Feature	Windows NT Server 4.0	Windows 2000 Server
Scalability without Complexity	Supports over 20,000 users per domain (partition).	Supports millions of objects per domain (partition). Active Directory uses indexed data store for fast retrieval. Optimized replication between sites and over slow network links. Global Catalog provides unified view of directory objects in multiple domains, and is updated simultaneously with other replication cycles to ensure low latency. Single data store and access methods for partitions and catalogs.
Internet Standards support	Not available.	Implemented as a native LDAP server that requires no request translation. Consistent interpretation of access control rights when access is via LDAP. Provides LDAP-based access to all features. Full namespace integration with DNS to simplify object location and access.
Flexible Security Services	Centralized management of user and group security.	Provides support for popular security technologies such as Kerberos and Smart Cards. Catalog enforces object- and attribute-level security. No restrictions on security groups that span domains.
Support for Synchronization and Consolidation	Primary domain controller contains a read/write version of the directory, while a backup domain controller contains a read only replica of the master database.	Provides the scalability required to consolidate large directories without administrative complexity. Built-in LDAP-based change history interfaces facilitate use as a meta-directory platform. Catalog architecture enables fast, efficient query of large number of objects.

Management Presentation Services	Graphical interfaces make it easy for administrators to manage Windows NT 4.0 networks. Windows NT Option Pack offers services such as Internet Information Server, Transaction Server, and Indexing, and can be managed using the MMC.	MMC is a single interface for viewing network functions and using administrative tools. Easy customization for task-based administration and logical grouping of tools.
Instrumentation Services	Supports Windows Management Instrumentation (WMI) as an add-on in Service Pack 4. WMI provides a standard interface to data generated by SNMP, DMI, the registry and other management interfaces.	Provides detailed application and data management across different vendors' products. Consolidates and unifies data provided by existing management technologies. Does not require specific APIs.
Group Policy Management	Operating system policies and settings can be defined using the Systems Policy Editor.	Group Policy Editor allows policies to be set on users and groups in a site, domain or OU in the Active Directory. Automates such tasks as operating systems updates, application installation, user profiles and desktop system lockdown. Granular assignment of policies to groups of users.
User Data Management	Using user profiles settings, local documents can be automatically synchronized with secure network copies	Users can roam any Windows 2000 Professional-based PC on the network and always have access to their data, applications and computer preferences. Users can also take key network-based resources offline, which will automatically synchronize upon reconnecting to the network.
Software Installation and Maintenance	Available with Microsoft Systems Management Server (SMS).	Administrators can specify a set of applications that will always be available to a user or group of users. If a required application is not available when needed it will automatically be installed. Auto-repair update and application removal are also supported.
User Settings Management	Available through the Zero Administration Kit (ZAK).	Centralized administration and control of desktop computers, with the ability to lockdown desktop configurations.

Remote Operating System Installation	Not available.	Using standards-based remote boot technology (PXE) a PC can automatically connect to a Windows 2000 Server and Install Windows 2000 Professional.

Table A.5. Security Services. After Ref. [30]

Feature	Windows NT Server 4.0	Windows 2000 Server
Security Configuration and Analysis (Security Configuration Editor)	Provided through the Security Configuration Editor in Service pack 4.0 for Windows NT Server 4.0. Automated configuration of various global and local security settings including security-sensitive registry settings, access controls on files and registry keys, and security configuration of system services. Security Configuration Editor allows administrators to define security configurations as a template to be applied to selected computers in one operation.	Adds policy based security management and configuration integrated with Active Directory.
Authentication	Support for multiple forms of authentication (user name/password, Web standards, etc). Offers single logon services.	Support for multiple forms of authentication (user name/password, smart card, Web standards, etc). Built-in support for standard, interoperable security protocol (Kerberos). Mutual authentication of both client and server. Faster performance through reduced server load during connection establishment. Support for delegation of authorization from clients to servers through the use of proxy mechanisms.
Public Key Certificate Services	Administrators given ability to set up a public key infrastructure (PKI) with the installation of Option Pack 4.0. Administrators could use the certificate server to issue certificates to users, who could then authenticate themselves through the built-in Internet Information Server (IIS). The certificate could be mapped to a Windows NT-based user account so access control could be managed through Windows NT access control lists (ACLs).	Built-in Public Key Certificate Server and support for third-party certificate authority (CA) services. Integrated support for public key (X.509) security with built-in infrastructure for smart card usage (logons, certificate storage and revocation) for Extranet security.

Smart Card Infrastructure	Third-party support.	Standard model for interfacing smart card readers and cards with PCs. Device-independent APIs for enabling smart card-aware applications. Familiar tools for software development. Broad support from all the leading smart card hardware vendors.
IP Security Protocol	Not available.	Support for IETF standard IP Security protocol for encrypting TCP/IP traffic. Tight integration of IPSec with a system policy management to enforce encryption between systems transparently to the end user. Used to secure communications within and intranet and to create VPN solutions across the Internet.
Encrypting File System (EFS)	Not available.	EFS built-in to NTFS as an integrated system service, making it easy to manage, difficult to attack and transparent to the user. Encryption technology used is public key-based. Enabled on a per-file or per-directory basis.

Table A.6. Application Services. After Ref. [30]

Feature	Windows NT Server 4.0	Windows 2000 Server
Support for large amounts of memory	Windows NT Server Enterprise Edition 4.0 introduced 4 GB memory tuning feature to give applications access to up to 3 GB of memory for improved performance. Intel provides a driver that allows customers to configure Windows NT Server 4.0 to support greater than 4 GB of memory on Intel Xeon-based servers.	Enterprise Memory Architecture (EMA) allows applications that perform transactions processing or decision support on large data sets to keep more data in memory for greatly improved performance. Support for greater than 4 GB physical memories on Compaq Alpha and Intel Pentium II Xeon systems. Depending on the specific platform, physical main memory sizes as large as 64 GB can be supported.
SMP Scalability	Provides support for up to 32 processors.	Optimized for a growing number of competitively priced eight-way and larger SMP servers based on ever-faster RISC and Intel Architecture processors.
CPU Management Services	Not available.	Job objects are namable, securable, sharable objects that control attributes of the processes associated with them. A job objects basic function is to allow groups of processes to be managed and manipulated as a unit.
Clustering Services	Windows NT Server 4.0 Enterprise Edition provides clustering services for high availability as well as IP load balancing.	Standard feature of Windows 2000 Advanced Server. Allows two servers to be connected into a cluster for higher availability and easier manageability. Broad industry support from hardware and software vendors. Open APIs for clustering enabling applications. Failover of operating system services and applications. Fine-grained control over application workloads partitioned between nodes.

Component Services	Microsoft Component Object Model (COM) and Distributed Model (DCOM) provide developers with a language neutral approach to building and deploying distributed applications.	Adds enhanced component services with automatic load balancing.
Transaction Services	Component-based middleware for quickly building scalable, manageable distributed transaction applications. Provides data integrity when updating one or more data sources, such as Oracle, Microsoft SQL Server, DB2, etc.	Transaction Services is a Windows 2000 Server feature that makes it easier to develop and deploy server-centric applications. Ideal for developing line-of-business and electronic-commerce applications with Web-based interfaces. Transaction Services works with COM+ and offers comprehensive component functionality, such as automatic transaction support for data integrity protection, simple but powerful role-based security, access to popular databases, message queuing products, and mainframe-based applications. It also includes performance-enhancing features such as connection pooling.
Message Queuing Services	MSMQ 1.0 is available for Windows NT 4.0 Server and Enterprise Edition. Store-and-forward middleware that provides assured delivery of messages between applications running on multiple machines across a network. Support for intelligent routing, automatic prioritization, easy manageability, and high-performance message rates. Integrated with Active Directory to make it easy to find queues over a network of computers.	The Message Queuing Services uses the Active Directory to store information about message queues. This allows applications to easily locate message queues across the network.

Table A.7. Web Services. After Ref. [30]

Feature	Windows NT Server 4.0	Windows 2000 Server
Process Accounting	Not available.	Provides information about how Web sites use CPU resources on the server. Process Accounting is enabled and customized on a per-site basis.
CPU Throttling	Not Available.	With the Job Object, administrators can limit the amount of CPU processing time a Web application can use over a predefined period of time.
Command-Line Management	Available with the Windows NT 4.0 Option Pack.	With Command-Line Administration, administrators can manage the Web services from the command line.
Remote GUI-Based Management	Available with IIS 2.0 - IIS 4.0	Windows 2000 Server provides a MMC Snap-in to manage the Web services from Windows-based systems.
Remote Browser-Based Management	Available with Windows NT 4.0 Option Pack.	Provides administrators with the ability to manage the Web services in Windows 2000 Server or individual web sites remotely from any Web browser that supports frames and JScript.
Host Multiple Web Sites on a Single Server.	Available with Windows NT 4.0 Option Pack.	Built-in, comprehensive multi-Web site support. Using the built-in support for HTTP 1.1 Host Headers, organizations can host multiple Web sites using a single IP address with Windows 2000 Server. HTTP 1.1 Web sites are also accessible to HTTP 1.0 downlevel clients. Administrators can also assign each Web site a unique IP address.
Virtual Directory Support	Available with all versions of IIS for Windows NT Server.	Provides a way for administrators to map long directory paths to shorter paths.
Per Web Site Bandwidth Throttling	Available with windows NT 4.0 Option Pack.	Administrators can manage the bandwidth allocation for each of the Web sites running on a single server.

Digest Authentication	Not available.	Offers the same features as Basic Authentication but involves a different way of transmitting the authentication credentials. The authentication credentials pass through a one-way process called hashing. The result is called a message digest (or hash) and cannot be decrypted. The original text cannot be deciphered from the hash.
Fortezza	Not available.	Satisfies the Defense Messaging System security architecture with a cryptographic mechanism that provides message confidentiality, integrity, authentication, and access control to messages, components, and systems.
FTP Restart	Not available.	If a user is interrupted when downloading a large file from an FTP site, the next time they download the file, it will start from where the user left off.
Integrated FTP Services	Available for all versions of IIS on Windows NT Server.	Windows 2000 Server provides customers with fully integrated FTP services.
W3C Logging Format	Available with the Windows NT 4.0 Option Pack.	Administrators can customize the logs generated by the Windows 2000 Server Web services by extending logged information.
Active Server Pages (ASP)	Available since IIS 3.0 for Windows NT Server 4.0	ASP is a framework for developing scalable business applications for the Web. ASP integrates with the Component Object Model to deliver distributed component-based applications to the Web.
Error Handling	Not available.	Using the new error handling capabilities for ASP, developers can trap errors in custom error messages. Developers can display useful information, such as an error description or the line number in an .asp file where the error occurred.
Index Services	Supported by Windows NT Server 4.0	Index Services also indexes the file systems, making finding files faster by searching on textual content.

APPENDIX B. MICROSOFT MANAGEMENT CONSOLE SNAP-INS.

The Microsoft Management Console (MMC) provides network administrators with a common console for viewing network functions and using administrative functions. Think of it as the "office water fountain" for network administrators - a place where administrators go to get all their information. MMC does not itself provide any management behavior, but provides the environment for administrative tools, called Snap-ins, to provide the actual management behavior. Microsoft and independent software vendors (ISVs) are designing Snap-ins for many of the features included in Windows 2000.

The following table includes many of the most useful Snap-ins already created. However, please keep in mind that this list is by no means complete - new Snap-ins are being written every day, and administrators can design their own Snap-ins to put in their "administrative toolbox" fairly easily.

Table B.1. MMC Snap-ins. After Ref. [31]

Snap-In	Description	Benefit
Computer Management	Designed as a computer configuration tool. It is designed to work with a single computer, and all its features can be used from a remote computer, allowing an administrator to troubleshoot and configure a computer from any other computer on the same network.	The Computer Management Snap-In is a remote Administrative Tools folder or remote toolbox. It not only provides access to the base Windows 2000 Server Tools (viewing events, creating shares, managing devices, and so on), but also dynamically discovers what server services and applications there are to administrate.
Device Manager and Hardware Wizard	Allows administrators to configure devices and resources on local computers.	Administrators can use the Hardware Wizard to add new hardware, change device properties, unplug or eject devices, and resolve hardware conflicts.
DHCP Manager	DHCP administration	Administrators can easily configure and manage DHCP services.
Directory Service Administration	The primary management tool for all objects located within the domain, including the User, Group, Contact and Computer.	Directory Service Administration provides basic functionality to create, modify, and delete objects and organization units, as well as the ability to move objects between organizational units.
Directory Service Migration Tool	Provides an architecture to discover NetWare resources, model them offline, and migrate them to Active Directory.	This migration tool ensures that the directory services will not be inadvertently corrupted during the migration because the offline copy on the local machine can be manipulated, changed, and updated as often as needed before migrating.

Disk Management	The Disk Management Snap-In is a graphical tool for managing disks that replaces the Disk Administrator found in Windows NT 4.0. It supports partitions, logical drives, and the new dynamic volumes. It contains shortcut menus and wizards to simplify creating volumes as well as initializing and upgrading disks.	This tool allows administrators to perform management tasks like creating, extending, mirroring a volume or even adding disks, all without rebooting the system of interrupting users.
Disk Defragmentation Utility	The Disk Defragmentation Utility reorganizes clusters on a disk volume so that files, directories, and free space are physically more contiguous. The Disk Defragmentation Utility will work with disk volumes that are formatted for FAT, FAT32, or NTFS file systems.	Depending on the extent of fragmentation, overall system performance can be improved significantly, as it relates to disk I/O, after the Disk Defragmentation Utility is executed.
DNS Manager	DNS is a distributed service, and in most cases, more than one computer acts as a DNS server.	The DNS Snap-in extends the Directory Service Administration and the Computer Management Snap-in because the DNS service itself needs to be configured on individual computers.
Domain Tree Manager	Administration of the Active Directory domain tree	
Event Viewer	Access to the three event logs	
File Service Management	Allows administrators to create shares and manage the sessions and connections on local or remote computers. It replaces functionality previously found in the System Control Panel application in Windows NT 4.0.	Used in conjunction with the Distributed File System (DFS), this tool could be used to connect together shares throughout the enterprise into a logical namespace. For example, users connect to one resource for access to all resources published within and DFS volume.
Folder	Establishes a directory in a specified place in the tree hierarchy	Provides a simple tool to create directories anywhere in the domain.

Group Policy Editor	The Group Policy Editor is the user interface for application deployment, policy options for computers and users, and scripts. It is responsible for managing the settings for Group Policy as it is applied to a given site, domain, or organizational unit. It also acts as an anchor point for third-party applications to build snap-in extensions or use .ADM files for managing application-specific policy.	Policy-based management will automate such tasks as operating system updates, application installation, user profiles, and desktop system lockdown.
Internet Service Manager (ISM)	Designed to allow administrators to quickly and efficiently manage IIS and other network applications and services from a single easy-to-use Windows-based interface.	Consolidates several separate applications into one Snap-In to present a common administrative tool.
IP Security Management	Administration of the encryption protocols on the IP level	IP Security Management governs end-to-end secure communication. Once an administrator has implemented IP security for an enterprise, communications are secured transparently; no user training or interaction is required.
Security Configuration Editor	The Security Configuration Editor is designed to manage and monitor overall system security, and to provide a central repository for security-related administrative tasks. With Security Configuration Editor, administrators will be able to use a common tool to configure and analyze security on one or more Windows 2000- and Windows NT-based machines in your network.	The Security Configuration Editor snap-in tool provides a graphical user interface that allows administrators to edit security configuration templates to define customized configurations. It also allows you to generate a template from settings in an existing system.
Site Replication Manager	Allows administration of the replication setup.	

System Service Management	Allows administrators to start, stop, pause, and resume services on local and remote computers. It replaces the Service Control Panel application in previous versions of Windows NT.	This feature allows the SCM service to manage common user problems, for example, when a service fails it can automatically restart the service, run a script or .exe file, or even reboot the server.
Systems Management Server	Systems Management Server is designed as a large series of integrated Snap-ins, which means that the administrator has the option of only taking part of the display offered by the console. For instance, a particular administrator may be responsible for software distribution—rather than providing them with the whole console including remote control, only the Snap-ins associated with software distribution are chosen. These Snap-ins are then put into their own console window and sent to this administrator who has exactly the tool set needed to do the specific task at hand.	Through this mechanism, different sets of administrators can be assigned different subsets of Systems Management Server easily and securely.

APPENDIX C. GLOSSARY OF TERMS AND ACRONYMS

ACE (Access Control Entry) -- Each ACE contains a security identifier (SID), which identifies the principal (user or group) to whom the ACE applies, and information on what type of access the ACE grants or denies.

ACL (Access Control List) -- A set of data associated with a file, directory or other resource that defines the permissions that users and/or groups have for accessing it. In the Active Directory directory service, an ACL is a list of access control entries (ACEs) stored with the object it protects.

Active Directory -- A structure supported by Windows 2000 that lets any object on a network be tracked and located. Active Directory is the directory service used in Windows 2000 Server and is the foundation of Windows 2000 distributed networks.

ADSI (Active Directory Service Interfaces) -- ADSI is a client-side product based on the Component Object Model (COM). ADSI define a directory service model and a set of COM interfaces that enable Windows NT and Windows 95/98 client applications to access several network directory services, including Active Directory.

API (Application Program Interface) -- A set of calling conventions defining how a service is invoked through a software package.

ASP (Active Server Pages) -- A Web programming technique that enriches Internet communications by improving script management. ASP files can execute with a transaction. Therefore, if the script fails, the transaction is aborted.

BDC (Backup Domain Controller) -- In a Windows NT Server 4.0 or earlier domain, a computer running Windows NT Server that receives a copy of the domain's directory database, which contains all account and security policy information for the domain. Backup domain controllers authenticate user logons and can be promoted to function as PDCs as needed. BDCs are not required in a Windows 2000 domain.

Authentication -- Verifying the identity of a user who is logging on to a computer system or verifying the integrity of a transmitted message.

Clustering -- Combining multiple systems to act as a single, redundant system.

COM (Component Object Model) -- Microsoft's groundwork of the ActiveX platform. Used to support interprocess communications and designed to promote software

compatibility. COM is an object-oriented programming model that defines how objects interact within a single application or between applications.

Container -- A special type of Active Directory object. A container is like other directory objects in that it has attributes and is part of the Active Directory namespace. However, unlike other objects, it does not usually represent something concrete. It is the container for a group of objects and other containers.

Cryptographic API (CryptoAPI) -- The Microsoft CryptoAPI provides an extensible architecture for developers to build exportable applications that take advantage of system-level certificate management and cryptography. Applications can use the functions in CryptoAPI without knowing anything about the underlying implementation, in much the same way that an application can use a graphics library without knowing anything about the particular graphics hardware configuration.

Cryptography -- Cryptography is the process of scrambling a message such that the message can be stored and transmitted securely. Scrambled, or *encrypted*, messages can achieve secure communications even when the transmission medium (i.e., the Internet) is not secure. One popular form of cryptography utilizes a method of both public and private keys. When using cryptographic methods, only the cryptographic keys must remain secret. The algorithms, the key sizes, and file formats can be made public without compromising security.

DFS (Distributed File System) -- A component of Windows 2000 Server that allows file shares to be maintained redundantly between multiple servers.

Digital Certificate -- An electronic identification and verification tool used to secure online commerce and other transactions.

Distinguished name -- Every object in the Active Directory has a unique distinguished name. The distinguished name identifies the domain that holds the object as well as the complete path through the container hierarchy by which the object is reached. A typical distinguished name might be: *CN=JamesSmith,CN=Users,DC=Microsoft,DC=Com*. This distinguished name identifies the "James Smith" user object in the Microsoft.com domain.

Domain -- A collection of hosts and routers, and the interconnecting networks, managed by a single administrative authority. A domain is a single security boundary of a Windows NT or Windows 2000 computer network. The Active Directory is made up of one or more domains. Every domain has its own security policies and security relationships with other domains.

Downlevel Domain -- A downlevel domain is a domain based on Microsoft technology released prior to Windows 2000. Windows NT 3.x - 4.0 domains are the most popular downlevel domains existing in today's networks.

EFS (Encrypting File System) -- Allows data to be encrypted on the NTFS disk media, making it impossible for someone to bypass the operating system to retrieve the information.

Extranet -- Refers to an intranet that is partially accessible to authorized outsiders.

Failover -- With clustering, when one server fails, a second server can automatically pick up the failed server's workload.

Forest -- A group of one or more Active Directory trees that trust each other. All trees in a forest share a common schema, configuration, and global catalog. All trees in a given forest trust each other via transitive bidirectional trust relationships.

FORTEZZA -- FORTEZZA is a term used to describe a family of security products, and is a registered trademark held by the National Security Agency. "FORTEZZA-enabled" or "FORTEZZA Certified" are terms applied to other hardware and software products that have had FORTEZZA security integrated. Examples include E-Mail, File Encryptors, WWW browsers, databases, digital cellular telephones, and routers.

FTP (File Transfer Protocol) -- A set of rules that allows two computers to talk to each other as a file transfer is carried out. This is the protocol used when you download a file to your computer from another computer on the Internet.

GC (Global Catalog) -- The global catalog contains a partial replica of every Windows 2000 domain in the directory. It lets users and applications find objects in an Active Directory domain tree given one or more attributes of the target object. The GC allows users to quickly find objects of interest without knowing what domain holds them and without requiring a contiguous extended namespace in the enterprise.

GUI (Graphical User Interface) -- The use of graphics rather than just words to represent the input and output of a program. Microsoft Windows 2000 is an example of an operating system that uses a GUI to interact with the user.

IETF (Internet Engineering Task Force) -- The IETF is a large, open international community of network designers, operators, vendors and researchers whose purpose is to coordinate the operation, management and evolution of the Internet and to resolve short- and mid-range protocol and architectural issues.

IIS (Internet Information Server) -- Microsoft IIS is a high-performance, secure, and extensible Internet server which enhances the functionality of Windows NT Server 4.0. and Windows 2000. A complete set of tools for building server-based Web applications is included in IIS. Another important feature of IIS is its Active Server Pages (ASP) capability, which allows Web authors to combine HTML, server-side scripts, and ActiveX controls.

IP (Internet Protocol) -- The network layer protocol for the Internet protocol suite.

ISAPI (Internet Services Application Programming Interface) -- ISAPI is a high-performance application-programming interface (API) for back-end applications for Microsoft Internet Information Server. A server-side interface, ISAPI offers significant performance advantages over the Common Gateway Interface (CGI), because it has its own dynamic-link library.

ISP (Internet Service Provider) -- A company which provides other companies or individuals with access to the Internet.

Kerberos -- A security system that authenticates users. Kerberos doesn't provide authorization to services or databases; it establishes identity at logon, which is used throughout the session. The Kerberos protocol is the primary authentication mechanism in the Windows 2000 operating system.

Key -- A value which must be fed into the algorithm used to decode an encrypted message in order to reproduce the original plain text. Some encryption schemes use the same (secret) key to encrypt and decrypt a message, but public key encryption uses a "private" (secret) key and a "public" key which is known by all parties.

KCC (Knowledge Consistency Checker) -- The KCC is a built-in service that runs on all domain controllers and automatically establishes connections between individual machines in the same site.

LAN (Local Area Network) -- A data network intended to serve an area of only a few square kilometers or less. Because the network is known to cover only a small area, optimizations can be made in the network signal protocols that permit data rates up to 100MB per second.

LDAP (Lightweight Directory Access Protocol) -- A protocol used to access a directory service. LDAP is a simplified version of the Directory Access Protocol (DAP), which is used to gain access to X.500 directories. Lightweight Access Directory Protocol is the primary access protocol for Active Directory.

Microsoft Certificate Server -- The Microsoft Certificate Server issues, revokes, and renews digital certificates. These certificates are used to identify users for subsequent authentication using public key technology. With certificates, clients can be assured of a server's identity.

MMC (Microsoft Management Console) -- A Windows-based tool that provides users with total management of all services and applications within a single utility. MMC itself provides no management behavior, but instead provides a common environment for the Snap-ins, which provide the actual management functionality.

MSC (Management Saved Console) File -- A "Management Saved Console" file that constitutes a tool. Once an administrator has assembled a tool using various Snap-ins, the administrator can save the tool to a .MSC file. The .MSC file persists the tool so that it can be opened and used again later. An .MSC file can be passed on to other administrators for use throughout a Windows NT or Windows 2000 domain.

Namespace -- A tree-formatted, ordered listing of all the nodes available in the current tool. The display of the namespace is similar to a folder and directory structure on a hard drive. The Active Directory is primarily a namespace, as is any directory service. A telephone directory is a namespace. The Internet uses a hierarchical namespace that partitions names into categories known as top-level domains such as .com, .edu, and .gov, which are at the top of the hierarchy.

NFS (Network File System) --A distributed file system developed by Sun Microsystems which allows a computer to access files over a network as if they were on its local disks. This file system has been incorporated in products by more than two hundred companies, and is now a de facto standard.

NetBIOS (Network Basic Input Output System) --The standard interface to networks on Windows NT systems.

Node -- Any manageable object, task, or view. Examples of nodes include computers, users, and web pages

Object -- Any user, system, resource, or service tracked within Active Directory. Attributes are used to describe objects, and hold data describing the thing that is identified by the directory object. Attributes of a user might include the user's given name, surname, and e-mail address.

ODBC (Open Database Connectivity) -- ODBC is a standard programming language interface that is used to connect applications to a variety of data sources. Access is generally provided through the Control Panel, where data source names (DSNs) can be assigned to use specific ODBC drivers.

OU (Organizational Unit) -- A container object that is an administrative partition of the Active Directory. OUs can contain users, groups, resources, and other OUs.

PKI (Public Key Infrastructure) -- PKI is a policy for establishing a secure method for exchanging information within an organization, an industry, or a nation. PKI is also an integrated set of services and administrative tools for creating, deploying, and managing public-key-based applications. It includes the cryptographic methods, the use of digital certificates and Certificate Authorities (CAs), and the system for managing the process.

PPTP (Point-to-Point Tunneling Protocol) -- A tunneling protocol for connecting Windows NT and Windows 2000 clients and servers over Remote Access Services (RAS). PPTP can be used to create a Virtual Private Network between computers running NT. It is an extension of PPP sponsored by Microsoft.

RADIUS (Remote Authentication Dial-in User Service) -- RADIUS is a dialup authentication and accounting protocol commonly used by Internet Service Providers (ISPs).

Schema -- The set of attributes available for any particular object type. The schema makes object classes different from each other. Schema information is stored within Active Directory, allowing administrators to add attributes to object classes and distribute them across a network.

Site -- A geographical location, as defined within Active Directory. Sites correspond to logical IP subnets, and can be used by applications to locate the closest server on a network.

SMP (Symmetric multi processing) -- Two or more similar processors connected via a high-bandwidth link and managed by one operating system, where each processor has equal access to I/O devices. The processors are treated more or less equally, with application programs able to run on any or perhaps all processors in the system, interchangeably, at the operating system's discretion.

Smart Card -- A smart card is an integrated circuit card (ICC) that is owned by either an individual or a group whose information must be protected according to specific ownership assignments.

Snap-In -- Software that makes up the smallest unit of console extension. One Snap-In represents one unit of management behavior (for example, the Windows NT event log viewer is a functional unit of management, and thus a good candidate to become a Snap-In).

SNMP (Simple Network Management Protocol) -- The network management protocol of choice for TCP/IP-based internets developed to manage nodes on an IP network.

Tool -- An assembly of multiple Snap-ins into a single console. A tool contains and provides all the management behavior represented by all the Snap-ins contained in the tool. A tool can be saved (in an .MSC file) and reloaded. A tool is also called a document.

Tree -- A single Active Directory domain.

UNC (universal naming convention) -- Used in Windows NT and Windows 2000 networking to completely specify a directory on a file server.

VPN (Virtual Private Network) -- The use of encryption to provide a secure connection through an otherwise insecure network, typically the Internet. VPNs are generally cheaper than real private networks using private lines but rely on having the same encryption system at both ends.

W3C (World Wide Web Consortium) -- The W3C was founded in 1994 to develop common standards and protocols for the World Wide Web, and produces free, interoperable specifications and sample code, along with reference materials for the World Wide Web.

ZAW (Zero Administration for Windows) -- An initiative within Microsoft that focuses on improving the Windows operating systems for maximum automation of administrative tasks with centralized control and maximum flexibility.

LIST OF REFERENCES

1. Kaplan, Ari and Nielson, Morten S., *NT 5: The Next Revolution*, The Coriolis Group, Inc., 1998.

2. Microsoft, "Introducing the Windows 2000 Servers," Internet (http://www.microsoft.com/windows/server/Overview/intro/introduce.asp).

3. Varhol, Peter D., *Windows NT 5.0: Microsoft's NT Strategy for Enterprise Information Systems*, p. 23-25, Computer Research Technology Corp., 1998.

4. Manes, Stephen and Andrews, Paul, *Gates: How Microsoft's Mogul Reinvented an Industry - And Made Himself the Richest Man in America*, Doubleday, 1993.

5. Microsoft, "A Brief History of the Windows NT Operating System Fact Sheet," Internet (http://www.microsoft.com).

6. Finnie, Scot and Patrizio, Andy, "Operating Systems: Windows for All Seasons," WinMag, July 1999, Internet (http://www.winmag.com/library/1999/0701/new0009.htm).

7. FastLane Technologies, "Getting Fit for Windows NT Server 5.0," white paper, June 1998, Internet (http://www.getreadyfor-nt5.co.uk/whitepaper.htm).

8. Northrup, Anthony, *Introducing Microsoft Windows 2000 Server*, Microsoft Press, 1999.

9. Microsoft, "Windows 2000 Server Overview," Internet (http://www.microsoft.com/ntserver/windowsnt5/exec/overview/overview.asp).

10. Thurrott, Paul, "SuperSite for Windows 2000 Windows FAQ," Internet (http://www.wugnet.com/wininfo/win2000/FAQ).

11. Microsoft, "Introducing Windows 2000 Advanced Server," Internet (http://www.microsoft.com/windows/server/Overview/intro/advanced.asp)

12. Compaq, "*Digital Clusters for Windows NT*," White Paper, Internet (http://www4.service.digital.com/clusters/index.asp)

13. Russinovich, Mark, "Inside Microsoft Cluster Server: Understand how this clustering solution works," *Windows NT Magazine*, p. 57-58, February 1998.

14. Microsoft, "What's New in Windows 2000 Advanced Server," Internet, (http://ww.microsoft.com).

15. Johnston, Stuart J. and Hayes, Mary, "Windows 2000: High-End Ambitions," *Windows Magazine*, April 1999, Internet (http://www.winmag.com/win2000/spotlight/1999/0401/041999iw_a.htm).

16. Microsoft, "Microsoft Windows NT Active Directory: An Introduction to the Next Generation Directory Service," white paper, 1997, Internet (http://www.microsoft.com).

17. Microsoft, "Microsoft Windows NT Server: Microsoft Management Console: Overview," white paper, 1996, Internet (http://www.microsoft.com).

18. Microsoft, Microsoft Internet Information Server Training Kit, Microsoft Press, 1998.

19. Microsoft, "Windows NT 5.0 Beta 1 Reviewer's Guide," white paper, September 1997, Internet (http://www.microsoft.com/ntserver).

20. Microsoft, "Distributed File System: A Logical View of Physical Storage," white paper, Internet (http://www.microsoft.com/ntserver).

21. Cone, Eric, K., Boggs, Jon, and Perez, Sergio, *Planning for Windows 2000*, New Riders, 1999.

22. Donald, Lisa and Chellis, James, *NT Server 4 in the Enterprise*, Network Press, 1997.

23. Microsoft, "Planning Windows NT Server 4.0 Deployment with Windows NT Server 5.0 in Mind," white paper, 1998, Internet, (www.microsoft.com/ntserver/).

24. Microsoft, "Windows 2000 Unattended Setup Parameters," Microsoft Technet CD-ROM for Quarter 4 1999.

25. Andrews, Paul, "Windows NT Strategy: Service Key to Growth," Seattle Times, Internet (http://www.seattletimes.com/news/business/html98/nt_072798.html).

26. Microsoft, "Secure Networking Using Windows 2000 Distributed Security Services," white paper, Internet (http://www.microsoft.com/Windows/server/Technical/security/DistSecServices.asp).

27. Microsoft, "Security Configuration Tool Set," white paper, Internet (http://www.microsoft.com/Windows/server/Technical/security/sctoolset.asp).

28. Microsoft, "Single Sign-On in Windows 2000 Networks," white paper, Microsoft Technet CD-ROM for Quarter 4 1999.

29. Microsoft, "An Introduction to the Windows 2000 Public-Key Infrastructure," white paper, Internet (http://www.microsoft.com/windows/server/Technical/security/PKIIntro.asp).

30. Microsoft, "Windows NT Server: Comparing Microsoft Windows NT Server to Novell Netware 5," Strategy white paper, Internet (http://www.microsoft.com/windows/server/Eval/comparison/NDSandNT)

31. Microsoft, "Management Services," Internet (http://www.microsoft.com/ntserver windowsnt5/exec/feature/MgmtServ.asp).

INITIAL DISTRIBUTION LIST

1. DEFENSE TECHNICAL INFORMATION CENTER 2
   8725 John J. Kingman Rd., STE 0944
   Ft. Belvoir, VA 22060-6218

2. DUDLEY KNOX LIBRARY 2
   Naval Postgraduate School
   411 Dyer Rd.
   Monterey, CA 93943-5000

3. DEAN DANIEL BOGER 1
   Chair, C3 Academic Group
   Naval Postgraduate School
   Monterey, CA 93943

4. MAJ MICHAEL CARAWAY 1
   CENTCOM J2 RSO
   1607 Hangar Loop Drive
   MacDill AFB, FL 33621

5. DAVID L. MORRIS 1
   HQ USCENTCOM
   CCJ2-RI BLDG 187
   7601 Hangar Loop Rd.
   MacDill AFB, FL 33621

6. PROFESSOR DOUGLAS E. BRINKLEY 1
   Department of Systems Management
   Code SM/Bi
   Naval Postgraduate School
   Monterey, CA 93943

7. PROFESSOR BRETT MICHAEL 1
   Department of Computer Science
   Code CS/Mb
   Naval Postgraduate School
   Monterey, CA 93943

8. LTCOL JOHN GIBSON 1
Department of Command, Control, and Communications
Code CC/Gj
Naval Postgraduate School
Monterey, CA 93943

9. JOHN MASKAVICH 1
BTG, INC
5100 West Kennedy BLVD
Suite 285
Tampa, FL 33609

10. EW1 (SW) THOMAS POUNDERS 1
589 Dyer Rd
Room 200A
Naval Postgraduate School
Monterey, CA 93943

11. LIEUTENANT DAVID R. OAKES 2
1816 Ellington Ct.
Valrico, FL 33594